

EXHIBIT A

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT DEPARTMENT
CIVIL ACTION NO.:

JANE DOE, INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY
SITUATED,

Plaintiff,

v.

BAYSTATE HEALTH SYSTEM INC.,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe (“Plaintiff”), individually and on behalf of the classes defined below, through their undersigned counsel, bring this Class Action Complaint against Baystate Health System Inc. (“Baystate” or “Defendant”), and allege as follows.

1. This is a class action arising from Defendant’s systematic violation of the privacy rights of its patients and website visitors by wiretapping the electronic communications of visitors to its website, <https://www.baystatehealth.org/> and <https://providers.baystatehealth.org/> (together, the “Baystate Website”), and violating patients’ rights to privacy with respect to their medical information.

2. During the relevant time period, Defendant’s Privacy Policy told patients and website users that: “Baystate Health (BH) is committed to protecting your privacy and *we have taken steps to protect your information*. We have designed our website (baystatehealth.org) to allow you to visit most areas *without identifying yourself* or supplying personal information. For those areas where you are requested to provide identifiable information, we assure you that *it will*

only be used to support your customer/patient relationship with BH.”¹ Defendant further states that “[a]t Baystate Health, we understand that your medical information is personal, and we are committed to maintaining the privacy of this information.”²

3. Defendant, however, intentionally used various digital marketing tools on its website that were able to identify the patients and website users on the Baystate Website, and purposefully and intentionally redirected patients’ and other Baystate Website users’ communications containing Personal Health Information (“PHI”) and other sensitive information to third parties. Defendant’s use of these re-routing tools caused Baystate Website users’ and patients’ Personally Identifiable Information (“PII”) and the contents of their communications through the website to be automatically disclosed to third parties in violation of patients’ and website users’ reasonable expectations of privacy, of their rights as patients, of their rights as citizens of Massachusetts, and of both the express and implied promises of Defendant.

4. Specifically, at all relevant times, Defendant disclosed information about its patients’ and website users’ communications—including their searches for medical information about conditions and procedures, the identities of their physicians, their requests to schedule appointments with physicians, registrations for support groups, patients’ request to log in to the patient portal, and when a patient clicks to make a telephone call in order to schedule an appointment with a specific doctor through the site—to Meta Platforms, Inc. (“Meta”) (formerly known as Facebook, Inc.) and/or Google without their knowledge, authorization, or consent.

5. Defendant’s conduct in disclosing patients’ and website users’ private health information and PII/PHI to Meta and Google violates Massachusetts law, including the Wiretap

¹ See <https://web.archive.org/web/20220622132503/https://www.baystatehealth.org/privacy-policy> (emphasis added).

² See <https://www.baystatehealth.org/notice-of-privacy-practices>.

Act, G.L. c. 272, § 99; G.L. c. 214, § 1B (Right to Privacy), and G.L. c. 111, § 70E (Patients' and Residents' Rights).

6. On behalf of herself and the alleged Classes, Plaintiff seeks an order enjoining Defendant from further unauthorized disclosures of her and Class members' personal information; awarding liquidated damages in the amount of \$1,000 per Website User Class member, general damages and benefit of the bargain damages for Patient Class members, attorneys' fees and costs; and granting any other equitable relief the Court deems appropriate.

PARTIES

7. Defendant Baystate Health, Inc. is a Massachusetts non-profit corporation with its principal offices at 759 Chestnut Street, Springfield, Massachusetts. Defendant touts that it is "a 716-bed independent academic medical center" and is "the community's major referral hospital," providing services that include: cancer care; critical care medicine; digestive disorder care; heart and vascular disease care; laboratory services; neurological disorders; obstetrics and gynecology care; and care for other injuries, illnesses, and conditions.³ Baystate designs and maintains, and/or directs the design and maintenance, of the Baystate Website from its offices in Massachusetts.

8. Plaintiff is an individual residing in Ludlow, Massachusetts. Plaintiff has visited the Baystate Website numerous times and has been treated by Defendant's physicians.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout Massachusetts and has its principal place of business in Springfield. G.L. c. 223A, §§ 2 and 3.

³ See <https://www.baystatehealth.org/locations/baystate-medical-center>.

10. Venue is proper in Hampden County pursuant to G.L. c. 223, sec. 8(4) because plaintiff resides in Hampden County and Defendant might sue or be sued in Hampden County. However, Plaintiff is seeking acceptance into the Business Litigation Session pursuant to Superior Court Administrative Directive 17-1 because this case is a consumer matter involving complex issues and cases based on similar claims have been assigned to the Business Litigation Session. *See Doe et al. v. Partners Healthcare System, Inc. et al.*, No. 1984CV01651, and *Doe v. Boston Medical Center Corporation*, No. 2384CV00326.

FACTUAL BACKGROUND

I. Massachusetts protects personal privacy.

11. Under G.L. c. 214, § 1B, all persons “have a right against unreasonable, substantial, or serious interference” with their privacy.

12. Patient health information is specifically protected by the law. The prohibitions against disclosing patient personal health information include prohibitions against disclosing PII/PHI such as patient names, IP addresses, and other unique characteristics or codes. Massachusetts law subjects medical providers who treat conditions such as substance abuse to heightened duties of confidentiality. G.L. c 111B, § 11.

13. Massachusetts law also protects residents from having the contents of their communications intercepted without their consent. Specifically, the Wiretap Act, G.L. c. 272, § 99, prohibits any person from willfully and secretly intercepting the contents of any wire communications through the use of any intercepting device unless given prior authority by all parties to a communication to do so.

14. As a health care provider, Defendant has common law and statutory duties to protect the confidentiality of patient information and communications with individuals regarding its services.

II. Defendant systematically violates its patients' and website users' privacy rights.

15. Defendant maintains the Baystate Website. The Baystate Website is designed for patients, prospective patients, and other website users to communicate with Defendant, including by allowing individuals to research doctors and request to schedule appointments with doctors, register for support groups, research health conditions and learn about related services offered by Defendant, learn about medical procedures offered by Defendant, and sign in to a personal patient portal called MyBaystate. Website users can use search bars on Defendant's website to type in the specific information, medical condition, medical procedure, type of doctor, or doctor that they want more information about.

16. Defendant provides medical care and serves Western Massachusetts and the so-called Knowledge Corridor Region of Massachusetts and Connecticut (including the greater Hartford-Springfield area).

17. Defendant knows that many of its patients reside in the state of Massachusetts and that its website is frequented by users who reside in Massachusetts or who seek its medical services in Massachusetts.

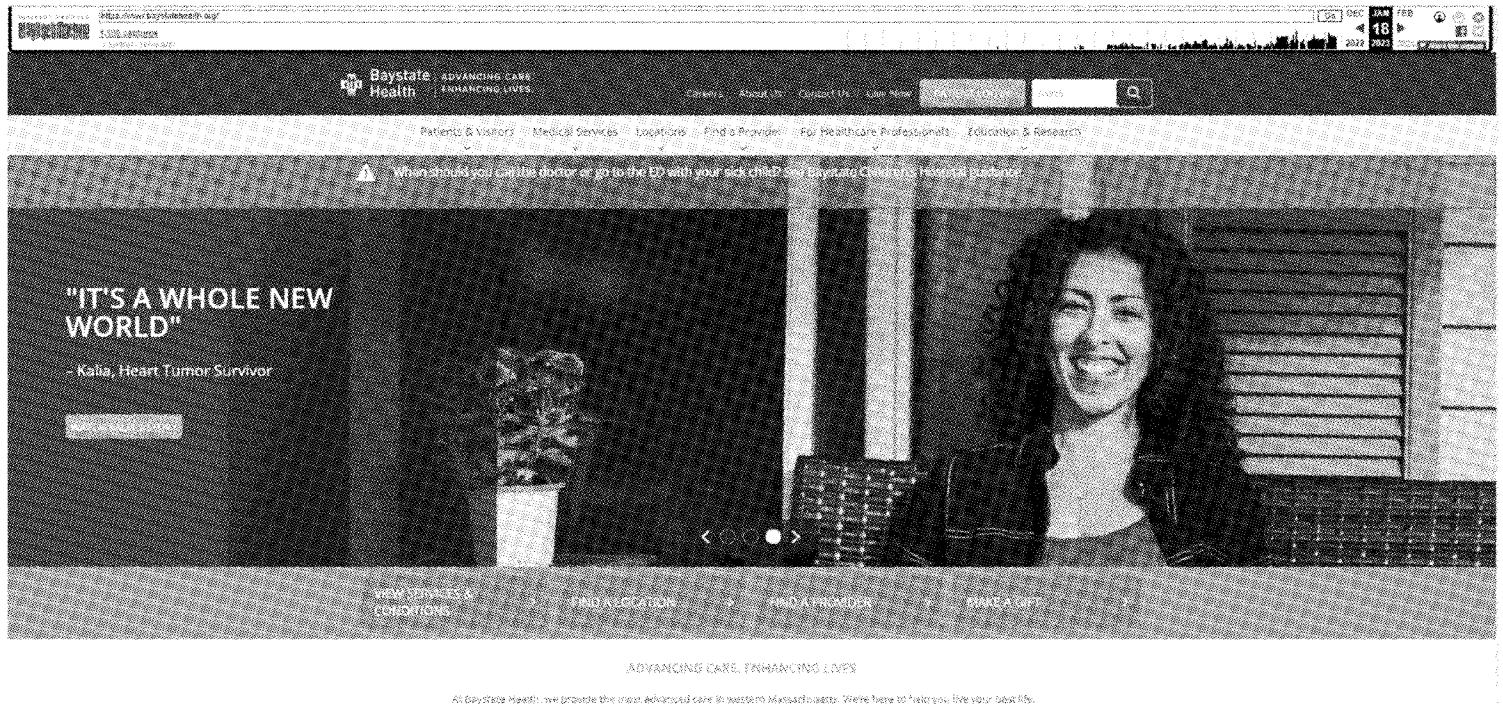
18. According to Joel Vengco, Vice President of Information & Technology and Chief Information Officer for Baystate Health, in or about the beginning of 2015, Defendant's website added "My Baystate Health," the online patient portal "that gives individuals access to portions of their medical records after they sign up."⁴

19. Below is an example of the top of the Baystate Website homepage as it appeared on January 18, 2023.⁵ As depicted, the homepage provides website users with tools to sign into

⁴ See <https://healthcarenews.com/think-tank-techspring-center-brings-silicon-valley-model-to-springfield/>.

⁵ See <https://web.archive.org/web/20221223120755/https://www.baystatehealth.org/>.

MyBaystate under the “Patient Log In” button, find a provider, explore medical services provided by Baystate and conditions that it treats, find a location, conduct a general search of the website, and more.



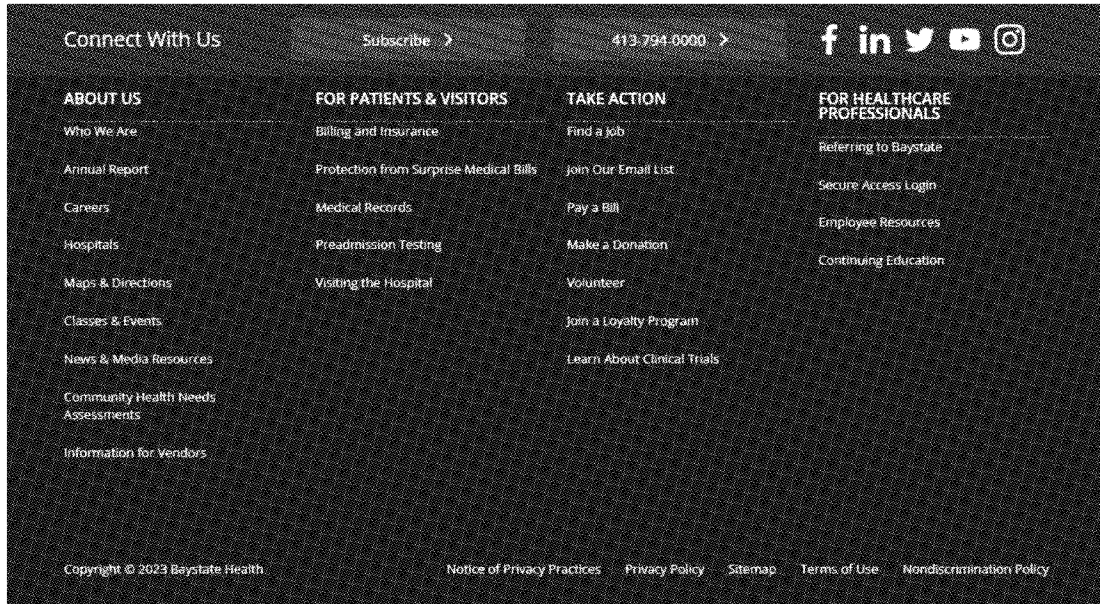
A. Patients and Website Visitors Reasonably Expect that Their Communications with Baystate on the Baystate Website Will Remain Confidential.

20. Defendant has statutory, regulatory, contractual, fiduciary, and common law duties to safeguard patients’ and website users’ PII and PHI from disclosure and ensure it remains private and confidential, and also expressly promises patients and website users that Defendant will maintain the confidentiality of patient information and communications and will use that information “only for your customer/patient relationship with Baystate Health.”

21. As displayed at the bottom of its homepage, Defendant provides patients and website visitors links to access Defendant’s Notice of Privacy Practices and Privacy Policy.

22. As shown below, Defendant’s Privacy Policy is located at the bottom of the Baystate Website in small font among several other links. Before it was last updated on May 15,

2023, Defendant stated in its Privacy Policy that “Baystate Health (BH) is committed to protecting your privacy. We have designed our website (baystatehealth.org) to allow you to visit most areas without identifying yourself or supplying personal information.”⁶ Defendant went on to promise that “We do not disclose your personal information unless the following conditions are met: · You provide to us a specific written consent, or · We are required by law.”⁷ Defendant also misleadingly



stated that “If you are browsing the BH web site, a cookie identifies only your browser!”⁸ As explained below, these promises of confidentiality and anonymity were illusory.

23. Defendant’s Notice of Privacy Practices is also located at the bottom of the Baystate Website. In it, Defendant states “At Baystate Health, we understand that your medical information is personal, and we are committed to maintaining the privacy of this information,” and links to the HIPAA Notice of Privacy Practices in both English and Spanish. HIPAA, short for the Health Insurance Portability and Accountability Act, is a federal law that establishes

⁶ <https://web.archive.org/web/20220622132503/https://www.baystatehealth.org/privacy-policy>.

⁷ *Id.*

⁸ *Id.*

national standards to protect individuals' medical records and other individually identifiable health information.

24. The HIPAA Notice is a two-page document entitled “Baystate Health Notice of Privacy Practices – Your Information. Your Rights. Our Responsibilities” (effective March 1, 2021).⁹ Those Privacy Practices explain:

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. If you have questions about this notice, please contact the Baystate Health Privacy Office at (413) 794-7955 or complianceoffice@baystatehealth.org. This notice describes the privacy practices of Baystate Health, Inc. (“Baystate”) and its affiliated entities.

Those Privacy Practices also provide numerous assurances for the privacy of information and Baystate’s responsibilities, including the following statements:

YOUR CHOICES:

For certain health information, you can tell us your choices about what we share. ...

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety. In these cases we never share your information unless you give us written permission:

- Marketing purposes
- Sale of your information

OUR RESPONSIBILITIES

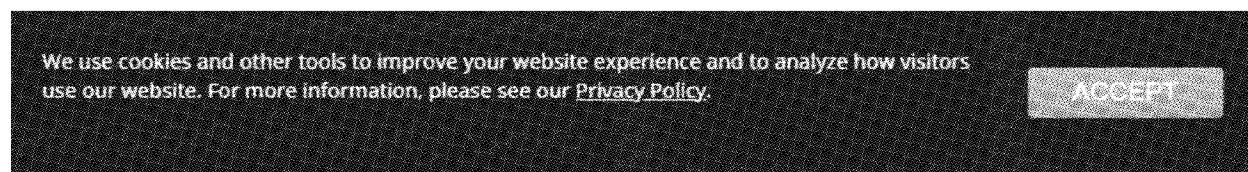
- We are required by law to maintain the privacy and security of your protected health information.

⁹ See <https://www.baystatehealth.org/-/media/files/about-us/corporate-information/hipaa-notice-of-privacy-practice-english.pdf?la=en>.

- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing.

25. These repeated promises by Defendant inform website users that they can use Defendant's website anonymously and that Defendant will not disclose PII/PHI and other sensitive information to third parties.

26. Moreover, before January 2023, Defendant's website did not feature any notification to patients and website users that cookies were used on the website. At some point in January 2023, Defendant began prompting patients and website users with the following "pop up" notification at the bottom of its homepage. There was no such warning and no prompt to "accept" the use of cookies on the Baystate Website before January 2023.



27. As described above, the Privacy Policy in January 2023 did not disclose to patients and website visitors that their communications on the website would be shared, along with PII, with third parties. The pop-up notification was therefore insufficient to obtain patients' and website users' consent to disclose their communications, PII, and PHI to third parties.

28. Despite these express promises and its legal duties, Defendant chose to share the content of its patients' and website users' communications with Meta and Google by intentionally installing tracking technology on the Baystate Website. Defendant disclosed the communications to Meta and Google without the knowledge or consent of website users or patients.

B. Defendant's Use of the Meta Pixel.

29. The Meta Pixel is a snippet of code, invisible to website users as they view a website, that tracks users as they navigate the web, logging which pages they visit, which buttons they click, and certain information they enter into forms or search requests.

30. Defendant began using the Meta Pixel by at least January 1, 2021. The presence of the Meta Pixel on Defendant's website can be shown using the Wayback Machine,¹⁰ as shown in the image below reflecting the code that Defendant installed on its website to enable the Meta Pixel on January 1, 2021.¹¹

```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(!f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://web.archive.org/web/20210101101705/https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '247095132483787');
  fbq('track', 'PageView');
</script>
<noscript>
  " "
</noscript>
<!-- End Facebook Pixel Code -->
```

31. Discovery will show that Defendant programmed the Meta Pixel to send information to Facebook about all website visitors—including Facebook users and non-Facebook users.

¹⁰ The Wayback Machine is a digital archive of the World Wide Web founded by the Internet Archive, a nonprofit based in San Francisco, California. Created in 1996 and launched to the public in 2001, it allows the user to go "back in time" and see how websites looked in the past.

¹¹ See <https://web.archive.org/web/20210101101705/https://www.baystatehealth.org/>.

32. The Meta Pixel sends information to Facebook via scripts running in a person's internet browser, so each data packet comes labeled with an IP address that can be used by Facebook in combination with other data to identify an individual or household.

33. An IP address is a number that identifies a specific device connected to the Internet and reveals geolocation. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), an IP address is considered PII (45 C.F.R. § 164.514(b)(2)(i)(0)).

34. If a website user is logged into Facebook when they visit a website that has installed the Meta Pixel, the communications can also be linked to a specific Facebook account which identifies a Facebook user's name, photo, and profile.

35. Facebook has over 2.9 billion active monthly users.¹² Facebook's Community Standards require users to use their real identities when signing up on the platform. This means users are only allowed one account and must use the name they use in "everyday life,"¹³ including first and last name.¹⁴ Users must also provide their birthday and gender.

36. When a user logs into Facebook using an internet browser, such as Google Chrome or Microsoft Edge, Facebook places several cookies on the user's browser.

37. A cookie is a piece of code placed on a browser by a server that contains information. A cookie can store different types of information, but the basic premise is to identify a) you and b) the website you visited that placed the cookie to begin with.

¹² See <https://www.reuters.com/technology/facebook-owner-meta-forecasts-q1-revenue-below-estimates-2022-02-02/>.

¹³ See https://transparency.fb.com/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fintegrity_authenticity.

¹⁴ See <https://www.facebook.com/help/229715077154790/>.

38. One of the cookies placed by Facebook on a user's browser upon login is the "c_user" cookie which contains the user's Facebook ID number. This cookie remains on a user's browser as long as they do not hit "Log Out" when they leave Facebook. Even if the person never visits Facebook.com using that browser again, the cookie will remain on the device for one year since the last visit to Facebook.

39. The long life of the c_user cookie is intentional—not only does the cookie allow Meta to identify users when they visit Facebook.com, it also allows Meta to track the user's activity across the web on the same browser. Because the Facebook ID is specific to a person, Meta can also match up a user's activity across devices using different browsers if that user has also logged in on another device.¹⁵

40. Website owners can also set additional Meta cookies, such as the "fr" or "_fbp" cookies and others, that unlike the c_user cookie, collect information on all website users—not just logged in Facebook users. Like the c_user cookie, these additional Meta cookies appear to contain unique identification numbers that are disclosed to Facebook along with the information tracked by the Meta Pixel, thereby permitting Facebook to target website users with personalized ads across different websites even if they are not Facebook users.

41. By tracking a specific person's movements across the web and across devices, Facebook collects enormous amounts of data regarding website users' interests, behavior, and connections.¹⁶ The quantity and quality of this data allows Meta to generate billions in advertising revenue—allowing businesses to target people with specific interests, target advertisements to specific people who visited their site but did not complete a purchase, and analyze the types of

¹⁵ See <https://www.facebook.com/business/news/cross-device-measurement>.

¹⁶ See <https://www.facebook.com/business/ads/ad-targeting>.

people that are visiting their site by leveraging user demographics, interests, and behaviors on other websites.

42. Businesses—like Defendant—access these services from Meta in part by installing the Meta Pixel on their website.

43. Pixels, also known as “web beacons,” are often small transparent images that an internet browser downloads like any other image on a website. When you visit a web page which contains the Meta Pixel, the pixel essentially contacts the Facebook ad server.

44. The business installing the pixel can program the pixel to record specific acts and communications, such as when a user places an item in their shopping cart, clicks a certain button, types in a search into a search bar, or otherwise interacts with the website.¹⁷ Meta receives the event information along with personal identifying information contained in the cookies described above.

45. The disclosures to Meta occur contemporaneously with communications between the website user and the website. The code causes the communications to be recorded on the user’s device and then transmitted in a package to Meta. By design, Meta receives the exact contents of the communications before the full response from the website has been rendered on the website users’ screen and while the communication between the website and the website user is ongoing.

46. If a business does not install the Meta Pixel, information on a user’s actions on the website would not be communicated to Meta.

47. Once the information is in the possession of Meta, Meta uses it for advertising and analytics purposes. Businesses know that Meta can identify the Facebook users visiting their website and track people who are not Facebook users across websites. The value for the business

¹⁷ See <https://developers.facebook.com/docs/meta-pixel/advanced>.

in programming their website with the pixel is derived from Meta's ability to identify the website visitors, track their behavior on their website, and link them to Meta data on their interests, behaviors, and connections, and to allow the business to target advertisements to specific users.

48. In some cases, a Facebook user can confirm that a website has shared information about their visit to that website with Meta via the Meta Pixel on a certain date by reviewing their "Off-Facebook Activity." Off-Facebook activity is "a summary of activity that businesses and organizations share with [Facebook] about [a user's] interactions, such as visiting their apps or websites."¹⁸ The Off-Facebook Activity report provided by Facebook to users, however, is an incomplete report of all activity on non-Facebook sites that has been shared with Meta by third parties such as Defendant.

49. On June 16, 2022, an article was published on The Markup titled "Facebook Is Receiving Sensitive Medical Information from Hospital Websites."¹⁹ The Markup is a nonprofit newsroom that investigates and publishes stories regarding technology. The article detailed how hospitals using the Meta Pixel were allowing the tracking tool to collect patients' sensitive health information, including details about their medical conditions, prescriptions, and doctor's appointments, along with users' IP addresses. As detailed by the article, several hospitals removed the Meta Pixel from the most sensitive parts of their websites, such as pages used to book appointments, or removed the Meta Pixel altogether after the article highlighted the privacy violations occurring.

50. After the Markup article was published, and as more and more lawsuits were filed against hospitals and healthcare providers for privacy violations related to the Meta Pixel,

¹⁸ See <https://www.facebook.com/help/2207256696182627>.

¹⁹ See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

Defendant likely recognized the privacy violations on its own website. Thus, as evidenced by the disappearance of the Meta Pixel code as viewable on the Wayback Machine, Defendant removed the Meta Pixel from its website by April 2023. Defendant also added the cookie pop up notification to its website in January 2023 and modified its Privacy Policy in May 2023 to add additional disclosures regarding the use of cookies.

C. Defendant's Use of Google Analytics.

51. Defendant began using Google Analytics by at least January 1, 2021. The presence of the Google Analytics code and other Google code can be shown using the Wayback Machine, as in the image below reflecting the code Defendant installed on its website to enable transmissions to Google from Defendant's website.

```
<!-- Google Tag Manager -->
<noscript>
  <iframe src="//web.archive.org/web/20210101101705if_/https://www.googletagmanager.com/ns.html?
    id=GTM-W988KP" height="0" width="0" style="display:none;visibility:hidden"></iframe>
</noscript>
<script>
  (function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
    new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
    j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
    '//web.archive.org/web/20210101101705/https://www.googletagmanager.com/gtm.js?
    id='+i+dl;f.parentNode.insertBefore(j,f);
  })(window,document,'script','dataLayer','GTM-W988KP');
</script>
<!-- End Google Tag Manager -->
```

52. Defendant also installed Google Analytics code on <https://providers.baystatehealth.org/>, the part of its website where patients can search for doctors and request appointments with specific doctors.

53. Defendant sends patient information to Google using Google Analytics, a web analytics service, which allows website owners to track visitor actions on their website and measure the effectiveness of advertising. Specifically, Defendant uses technology such as Google

tag manager and cookies to send the contents of website users' and patients' communications with the Baystate Website and IP addresses to Google.

54. Google Analytics automatically collects IP addresses of individual Internet users in order to facilitate and track Internet communications. However, Google Analytics offers website owners an opt-in IP anonymization feature. According to Google, this feature is designed to help site owners comply with their own privacy policies and the recommendations of data protection authorities. If the IP anonymization feature is enabled by the website owner, an additional parameter is added to the communications between website visitors' computers and the Google Analytics server, defined as `aip=1`. Accordingly, when the "aip" parameter does not appear, the IP address is not anonymized, enabling Google to identify a website user's IP address connected with their communications made via the website.

55. Baystate did not opt-in to Google Analytics' IP anonymization feature, as evidenced by the absence of the `aip=1` parameter on communications sent to Google from the Baystate Website.

56. Simply put, Defendant intentionally programmed Google Analytics in such a way as to disclose the content of website users' communications with the Baystate Website along with website users' PII/PHI in the form of IP addresses.

57. While Defendant has removed the Google code from <https://providers.baystatehealth.org/>, Defendant continues to use Google Analytics on <https://www.baystatehealth.org/> and to share patients' and website visitors' sensitive communications on that website with Google to this day.

D. The nature of defendant's intentional, unauthorized, unnecessary, and unlawful disclosures.

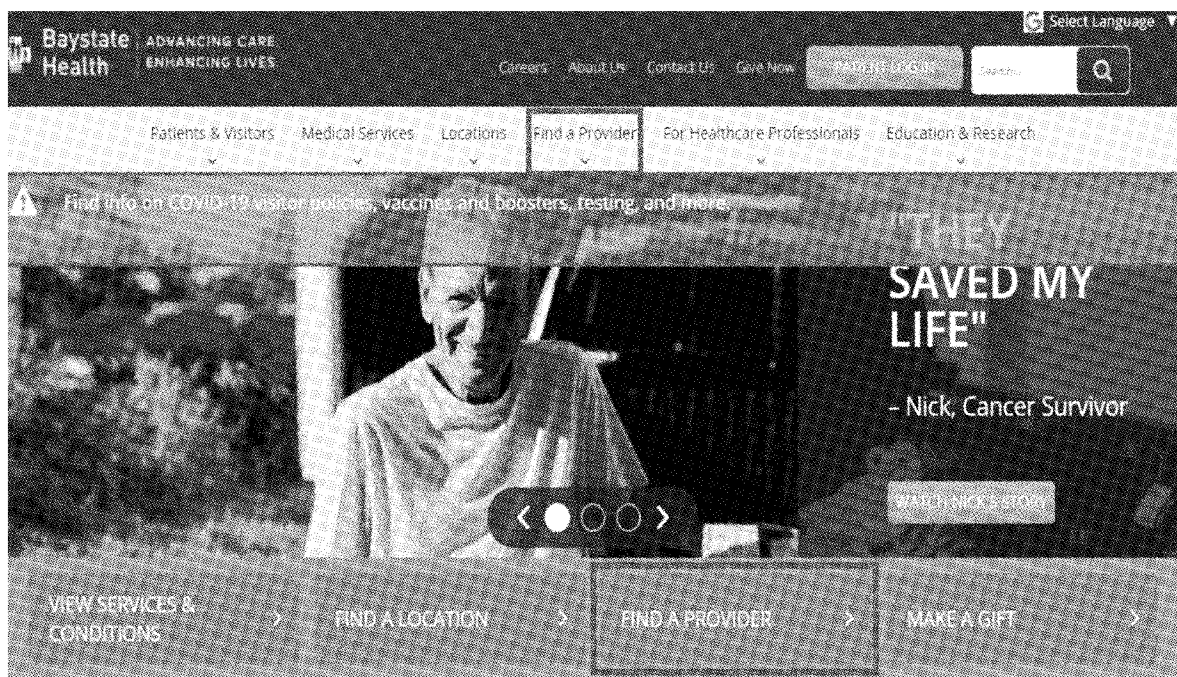
58. As intentionally implemented by Defendant, the Meta Pixel and Google Analytics tag causes PII/PHI, as well as the exact contents of the communications exchanged between Defendant and its website users and patients, to be sent to Meta and Google.

59. Defendant's third-party disclosures occur contemporaneously with communications by Plaintiff and Class members to Defendant's website.

60. By design, Meta and Google receive and record the exact contents of these communications before the full response from Defendant to Plaintiff or a Class Member has been rendered on the screen of the website users' devices and while the communications between defendant and website users remains ongoing.

61. Defendant installed the Google and Meta code on its website in a way that enabled transmissions from across Defendant's website, not just the web pages detailed herein. Discovery will show the full scope of Defendant's disclosures to Meta and Google. The examples provided below are for illustrative purposes only and do not attempt to describe the full scope of Defendant's privacy and wiretap violations.

62. When a website user clicks on the “Find a Provider” links provided by Defendant on the home page, they are directed to <https://providers.baystatehealth.org/>, where Defendant installed the Google tracking technology.



63. At this website, patients can navigate to a page providing a list of doctors and where they are able to search for a doctor by name, condition, specialty, location, gender, language, and more.

What do you need help with today?

Enter a Condition, Specialty, or Provider Name

1953 providers found

Distance: Within 25 miles

City, State or ZIP

Specialties: Choose Specialty

Locations: Type Here...

Online Scheduling: Book Online (101)

Pamela Jean Behrens, CNP
 VIRTUAL VISITS AVAILABLE
 4.8 out of 5 (87 ratings)
 Specialties: Urogynecology
 Affiliations: Baystate Medical Center
 Practice Locations: Baystate Urogynecology, Tolosky Center, 3300 Main Street, Suite 4B, Springfield, MA 01199 (Map)
 Phone: 413-795-8764

Catherine Henry Tipton, CNP
 ACCEPTING NEW PATIENTS VIRTUAL VISITS AVAILABLE
 4.9 out of 5 (62 ratings)
 Specialties: Surgical Oncology
 Affiliations: Baystate Medical Center, Baystate Noble Hospital
 Practice Locations: Baystate Medical Practice

64. As shown in the image to the right, patients can enter the parameters they would like to use to search for a doctor. When a patient entered the parameters, Defendant disclosed the parameters and search terms used by patients and website users to Google.

65. After a patient or website user conducts a search for a provider, Defendant displays a list of doctors that meet the search criteria, such as the list shown below.

Distance: Within 25 miles

Springfield, MA, USA

Specialties: Infectious Diseases

Baystate Medical Practice Provider

Show only (2)

Affiliations: Baystate Franklin Medical Center (2), Baystate Medical Center (2), Baystate Noble Hospital (2), Baystate Wing Hospital (1)

Age Groups Seen: Adults (2)


Accepting New Patients: Yes (2)

Provider Gender: Female (2)

Language: English (2)

3 providers found near Springfield, MA
01199, USA [Clear Filters](#)

Best Match | Availability | Distance | A-Z | Z-A



Megan C. Gallagher, MD

ACCEPTING NEW PATIENTS


VIRTUAL VISITS AVAILABLE

Specialties
Infectious Diseases

Affiliations
Baystate Franklin Medical Center
Baystate Medical Center
Baystate Noble Hospital
Baystate Wing Hospital

Practice Locations

	Phone	Distance
Baystate Infectious Disease 759 Chestnut Street, Springfield, MA 01199 (Directions)	413-794-7394	0.08 miles
Baystate Infectious Disease Tolosky Center, 3300 Main Street, Suite 3C, Springfield, MA 01107 (Directions)	413-794-7394	0.21 miles



Claire E. Magauran, MD

ACCEPTING NEW PATIENTS

VIRTUAL VISITS AVAILABLE

Specialties
Infectious Diseases
HIV Medicine

Affiliations
Baystate Franklin Medical Center
Baystate Medical Center
Baystate Noble Hospital


Practice Locations

	Phone	Distance
Baystate Infectious Disease 759 Chestnut Street, Springfield, MA 01199 (Directions)	413-794-7394	0.08 miles

66. Patients and website users can then select a doctor that they are interested in.

Once patients or website users select a doctor, Defendant also sent this information to Google.

[Return to search results](#) or [Start a new search](#)



Megan C. Gallagher, MD
Infectious Diseases

ACCEPTING NEW PATIENTS

VIRTUAL VISITS AVAILABLE

[Schedule Appointment](#)

[About](#) | [Expertise](#) | [Insurance](#)

About Megan C. Gallagher

Provider Gender Female

Language English

Age Groups Seen Adults

Practice Groups Baystate Infectious Disease

67. For example, as shown below, when a patient searches for a female doctor who specializes in infectious diseases for adults and accepts patients in Springfield, specifically in

Franklin Medical Center and speaks English, and then enters Dr. Megan C. Gallagher's profile page, Defendant sent all of this information to Google along with the patient's IP address.

Request URL: https://www.google-analytics.com/collect?v=1&_v=j96&a=503509314&t=timing&s=2&dl=https%3A%2F%2Fproviders.baystatehealth.org%2Fprovider%2F%2F759071%3Fdisplay_location%3D%3D%252C%2520VA%252C%2520USA%26distance%3D0%26filter%3Dspecialties.specialty.untouched%253A%253AInfectious%2520Diseases%26filter%3Dnetwork_affiliation.s.name%253ABaystate%2520Franklin%2520Medical%2520Center%26filter%3Dage_groups_seen.name%253AAdults%26filter%3Dgender%253AFemale%26filter%3Dlanguages.language%253AEnglish%26location%3D38.7892301%252C-77.1672035999999%26from%3Dsearch-list&ul=he-il&de=UTF-8&dt=Dr.%20Megan%20C.%20Gallagher%2C%20MD%20-%20Springfield%2C%20MA%20-%20Infectious%20Diseases%20-%20Schedule%20Appointment&sd=24-bit&sr=1920x1080&vp=1472x961&je=0&pit=3803&pdt=3803&ds=207&rnt=3&srt=965&tcp=403&dit=2622&clt=2622&_gst=16258_gbt=1702&_cst=16266_cbt=16948_u=SDCACFA68AAAAC-&jid=&gid=&cid=1424047393.1654590285&tid=UA-9927205-1&_gid=498425997.1654590285>n=2wg60PBQn48F&z=1321256630

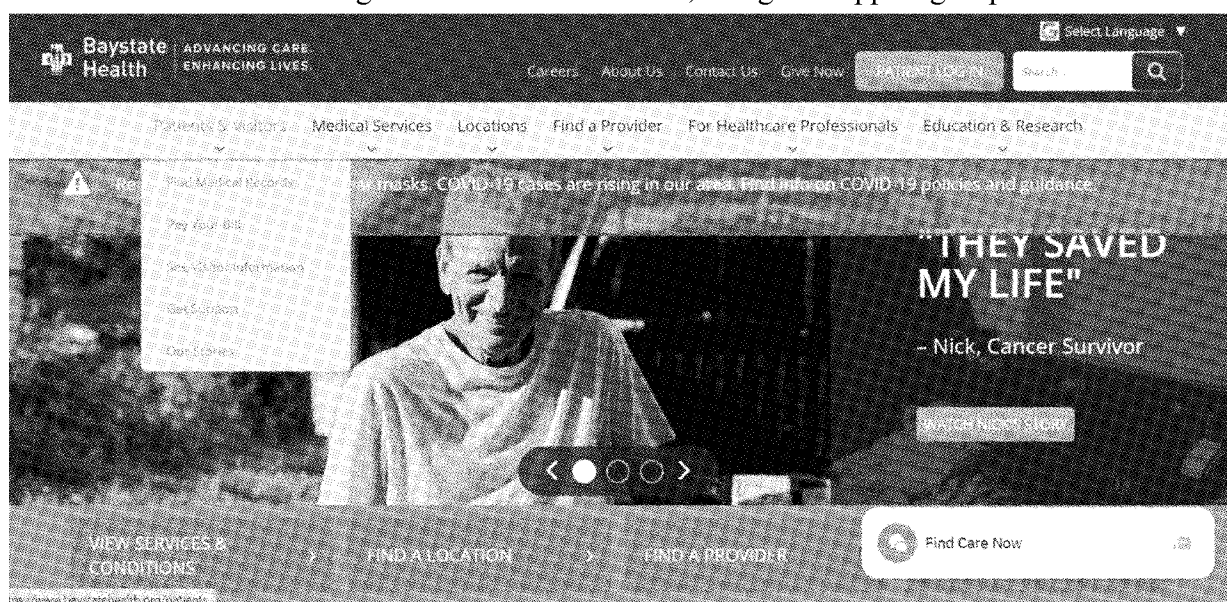
68. Defendant offers patients and prospective patients the option to schedule an appointment with a doctor from the provider search results page and on the doctor's profile page, as reflected in the green "Schedule Appointment" buttons in the images above.

69. The fact that a person is a patient of a medical provider is PHI under HIPAA.

70. For example, as shown below, when a patient clicks the "Schedule Appointment" button, Defendant disclosed to Google that the patient was scheduling an appointment with a specific doctor, the search that led the patient to that specific doctor, and again the patient's IP address.

Request URL: https://www.google-analytics.com/collect?v=1&_v=j96&a=499566268&t=event&ni=0&_s=7&dl=https%3A%2F%2Fproviders.baystatehealth.org%2Fsearch%3Fdisplay_location%3D%3D%252C%2520VA%25201199%252C%2520USA%26distance%3D0%26filter%3Dnetwork.s.network%253AEmployed%2520Network%26filter%3Dspecialties.specialty.untouched%253AInfectious%2520Diseases%26filter%3Dnetwork_affiliations.name%253ABaystate%2520Franklin%2520Medical%2520Center%26filter%3Dnetwork_affiliations.name%253ABaystate%2520Medical%2520Center%26filter%3Dage_groups_seen.name%253AAdults%26filter%3Dgender%253AFemale%26filter%3Dlanguages.language%253AEnglish%26filter%3Dnetwork_affiliations.name%253ABaystate%2520Noble%2520Hospital%26location%3D42.1208719%252C-72.6029199%26sort%3Dnetworks%252Crelevance&ul=en-us&de=UTF-8&dt=Dr.%20Megan%20C.%20Gallagher%2C%20MD%20-%20Springfield%2C%20MA%20-%20Infectious%20Diseases%20-%20Schedule%20Appointment&sd=24-bit&sr=1920x1080&vp=1286x961&je=0&ec=user_action&ea=user_action.cta&el=user_action.cta&_u=NjCICEF6BAAAAC-&jid=&gid=&cid=1332328207.1649685651&tid=UA-9927205-1&_gid=1722676519.1650185520>n=2wg4d0PBQn48F&z=1051408031

71. On <https://www.baystatehealth.org/>, Defendant offers patients the option to participate in various support groups. Patients are able to click the "Patients & Visitors" button on the main page and choose "Get Support", or search for a specific event through the search bar. Support groups offered include, for example, a virtual weight loss surgery support group which is open to patients enrolled in Baystate Health's bariatric surgery program, cancer support groups which are open to those who have been diagnosed with cancer, breast cancer support groups open to those who have been diagnosed with breast cancer, and grief support groups.



72. Information relating to past, present, or future physical or mental health or condition of an individual including specific diagnoses, is PHI under HIPAA.

73. Defendant's website allows patients and website users the ability to register for support groups on the website.

JOURNEY THROUGH GRIEF SUPPORT GROUP

Please join us for a weekly bereavement support group.

JOURNEY THROUGH GRIEF

Journey Through Grief is a weekly bereavement support group for adults who are struggling with the loss of a loved one. Registration is required. The group is free of charge.

This educational support group will provide materials and information on the grieving process, so as to better understand the grief experience and gather tools to cope with loss.

Wednesday, 10 - 11 am

January 16 - March 5, 2019

350 Main St, 4th Floor, Room # 489

Springfield, MA

To register please call or email, Betsy Flores, Bereavement Coordinator. Betsy's contact at 413-784-5559 or betsy.flores@baystatehealth.org



74. However, when a patient or website user clicks the “Register” button, Defendant sends this information to Meta and Google along with the patients’ IP address and identifying Facebook cookies.

```
Request URL: https://www.google-analytics.com/collect?v=1&_v=j96&ae=1184811751&t=event&ni=0&_s=1&dl=https%3A%2F%2Fwww.baystatehealth.org%2Fabout-us%2Fcalendar%2Fspiritual-services%2Fjourney-through-grief&ul=en-us&de=UTF-8&dt=Journey%20through%20Grief%20%7C%20Baystate%20Health&sd=24-bit&sr=1920x1080&vp=1196x961&je=0&ec=mailto&ea=Register%20button&el=https%3A%2F%2Fwww.baystatehealth.org%2Fabout-us%2Fcalendar%2Fspiritual-services%2Fjourney-through-grief&_u=5C6A1EA98-4jiid=&gjid=&cid=1332328207.1649685651&tid=UA-9827205-1&_gid=126151795.1651479983&gtn=2wg4r0w988KP&cgl=Service%20Line&z=1062919632
```

75. Defendant also allows patients and website users to request specific information by submitting requests in the search bar provided at the top of the home page. Patients and website users can search for doctors, information about conditions that Baystate Health treats, treatment options, and more.

76. Defendant disclosed to Meta and Google the text of the searches typed into the search bar by patients and website users, along with their IP addresses and other PII.

77. As also shown in the images above, next to the search bar on the home page, Defendant provided a green “PATIENT LOG IN” button to patients. This button directs patients to <https://mybaystate.baystatehealth.org/#/login>, where they can log in to the patient portal and access medical records, make payments, view appointments and make appointments, and more.

The button was provided by Defendant throughout the Baystate Website and other links to the patient portal were provided to patients as well, such as on the medical records page:

<https://www.baystatehealth.org/patients/medical-records>.

78. The fact that a person is a patient of a medical provider is PHI under HIPAA.

79. When a patient clicked this button or the other links provided to the MyBaystate portal login page, Defendant programmed its website to disclose to Google the information highlighted below, which contains the fact that the patient was requesting to log in to the patient portal, along with PII such as their IP address. The code shown below is visible using the WayBack Machine to interact with the page as it was during the relevant time period:

```
https://web.archive.org/web/20190801140235/https://www.google-analytics.com/r/collect?v=1&_v=j77&
a=789417493&_t=event&_ni=0&_s=1&dl=https%3A%2F%2Fwww.baystatehealth.org%2Fpatients%2Fmedi
cal-records&ul=en-us&de=UTF-8&dt=Medical%20Records%20%7C%20Baystate%20Health&sd=24-bit&
sr=1920x1080&vp=1718x1034&je=0&fl=32.0%20r0&ec=Outbound&ea=Click&el=https%3A%2F%2Fmy
baystate.baystatehealth.org%2F%3F_ga%3D2.222881438.460604823.1657167446-1194375229.165716744
6%23%2Flogin&_u=aGDACEABB~&_gid=154672583&_gjid=249462703&_cid=1194375229.1657167446&_tid
=UA-9927205-1&_gid=460604823.1657167446&_r=1&gtm=2wg7o0W98BKP&z=105919696
```

80. These third-party disclosures were made by Defendant without the website users' or patients' knowledge, consent, or any affirmative action taken. As described above, Defendant does not provide any information to patients or website users that would alert them to the fact that the contents of their communications on the Baystate Website are disclosed to Meta and Google. In fact, Defendant misled patients and website users to believe that they can use the website confidentially.

III. Defendant chose to make the disclosures to enrich itself.

81. Defendant is not required to make disclosures to Meta or Google in the ordinary course of business. The Baystate Website and services can function without the code that Defendant installed on the Baystate Website to enable the interceptions, as evidenced by Defendant's removal of the tracking code from many places on the website. For example, the

disclosures are not necessary for Defendant to maintain a website or use social media marketing tools.

82. It is possible for Defendant to allow patients to search for information about their health conditions and find doctors without disclosing those searches to third parties. It is also possible for Defendant to allow patients to schedule appointments with providers and register for support groups without disclosing those communications to third parties.

83. Despite these facts, Defendant affirmatively chose to provide Meta and Google secret and invisible “windows” that allowed them to record the exact contents of patient and website user communications on the Baystate Website and PII/PHI.

84. Defendant chose to install the tracking technology on the Baystate Website for marketing and/or analytics purposes. In exchange for PII/PHI about Defendant’s patients and website users, Meta and Google use the information to provide enhanced online advertising services and/or analytical services to Defendant.

85. Further, once the information is shared by Defendant with Meta and Google, Defendant loses the ability to further control the dissemination and use of the PII/PHI and the disclosed communications. Discovery will show that Meta and Google use the information disclosed by Defendant for their own purposes.

86. The monetization of the data disclosed by Defendant, both for its own purposes and those of the third parties, demonstrates the inherent value of the information collected.

87. By sending this sensitive information and communications to third parties, Defendant violates Plaintiff’s and Class members’ rights to privacy in that information and communications and their right not to have their PII and PHI shared without their knowledge or consent.

FEDERAL REGULATORY WARNINGS

88. On July 20, 2023, the Federal Trade Commission (“FTC”) and the U.S. Department of Health and Human Services’ Office for Civil Rights (“OCR”) issued a press release explicitly cautioning hospitals and telehealth providers, such as Baystate, about “the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers’ sensitive personal health data to third parties.”²⁰

89. In that press release, Samuel Levine, Director of the FTC’s Bureau of Consumer Protection admonished that:

When consumers visit a hospital’s website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers’ health information from potential misuse and exploitation.

90. The press release further advised that HHS and the FTC had “sent the joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user’s online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.”

91. In their letter to healthcare providers dated July 20, 2023, HHS and the FTC “reiterated the risks posed by the unauthorized disclosure of an individual’s personal health

²⁰ See <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.” *Id.*²¹

92. Indeed, as reported, “HHS highlighted these concerns in a bulletin it issued late last year that reminded entities covered by the Health Insurance Portability and Accountability Act (HIPAA) of their responsibilities to protect health data from unauthorized disclosure under the law.” Those admonitions even extended to companies not covered by HIPAA as providers “still have a responsibility to protect against the unauthorized disclosure of personal health information—even when a third party developed their website or mobile app. Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC’s Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC’s Health Breach Notification Rule.”

93. Earlier this year, in a March 16, 2023, the FTC Office of Technology issued a blog posting titled “Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking,” in which the FTC provided further cautionary warnings to about the use of pixel tracking, such as the Meta Pixel, and the serious privacy violations such tracking causes.²² In that blog, the FTC discussed its recent

²¹ A copy of the letter dated July 20, 2023, that was signed by the Director of HHS’s Office for Civil Rights, Melanie Fontes Rainer, and the Director of the FTC’s Bureau of Consumer Protection is available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

²² See <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>.

enforcement actions against GoodRx and BetterHelp, two digital healthcare platforms, for allegedly sharing user health data with third parties for advertising.

PLAINTIFF'S EXPERIENCE

94. Plaintiff Jane Doe has and had objectively reasonable expectations of privacy in communications with the Baystate Website that are grounded in her status as a patient of Defendant's, Defendant's legal obligations to maintain the confidentiality of wire communications and communications with patients, state and federal laws protecting the confidentiality of patient communications and medical information, and Defendant's express promises, as described above.

95. Plaintiff has been a patient of Defendant's for at least 10 years and is a current patient. Plaintiff regularly exchanged communications with Defendant on the Baystate Website during the relevant time period.

96. In the last few years, Plaintiff has communicated on the Website to obtain information related to breast cancer screenings and schedule a mammogram, to log in to the MyBaystate patient portal, and to search for providers.

97. Defendant disclosed Plaintiff's confidential communications with Defendant through the Baystate Website to Meta and Google.

98. Plaintiff has confirmed that Defendant disclosed her communications and sensitive information to Meta through the Off Facebook Activity Report. Plaintiff has been a Facebook user since at least 2010. Even though such reports provided by Facebook are incomplete, a report generated by Plaintiff captured approximately **80 disclosures** of Plaintiff's communications by Defendant to Meta between November 19, 2021 through April 10, 2023.

99. The presence of this data on the report confirms that the c_user cookie was present on Plaintiff's device and operating as Defendant intended when it installed it on the Baystate Website during the relevant time period.

100. Google cookies were also present on the device Plaintiff used to visit Defendant's website.

101. The demonstrated operation of the Facebook cookies on Plaintiff's device also indicates that the Google cookies supporting the Google tracking code installed by Defendant on the Baystate Website would also have operated as expected on Plaintiff's device during the relevant time period.²³

102. The sensitive information exchanged was disclosed along with PII/PHI regarding Plaintiff, such as her IP address, Facebook ID, and other unique identifiers.

103. Plaintiff was not aware that Defendant was disclosing her PII/PHI or the contents of her communications with the Baystate Website to Meta and Google and never consented to or authorized such disclosures.

104. Plaintiff was shocked when she discovered the privacy violations and is distressed that Defendant has been disclosing her private information to third parties without her knowledge or consent.

105. Plaintiff is a Massachusetts resident who was communicating with the Defendant, a Massachusetts corporation, and Defendant illegally caused these communications to be recorded in Massachusetts on Plaintiff's device before causing them to be automatically sent to a third party.

106. Discovery will show that Defendant disclosed the information regarding Plaintiff in exchange for enhanced marketing and analytical services from Meta and Google. Defendant benefitted from Plaintiff's information without ever intending to compensate Plaintiff or to inform her that the disclosures had been made.

²³ As noted the reports are incomplete and the absence of the data would not indicate that either the Meta cookies or Google cookies were not operating as expected on a given device.

107. Defendant violated Plaintiff's rights to privacy in her PII/PHI and sensitive, confidential medical communications.

108. Defendant's conduct injured Plaintiff and will continue to injure Plaintiff.

109. Defendant's disclosures to Google are ongoing.

110. Injuries to Plaintiff are also ongoing because her confidential and private information is now in the hands of Meta and Google who have used the information and can continue to use the information for their own purposes.

CLASS ALLEGATIONS

111. Plaintiff brings claims on behalf of herself, individually, and on behalf of the following classes:

The Website User Class

All Persons who, within the statute of limitations, exchanged communications with the Baystate Website and who (a) are a resident of Massachusetts, and/or (b) received medical care or advice in Massachusetts from Defendant.

The Patient Class

All Persons who, within the statute of limitations, were patients of Defendant and exchanged communications with the Baystate Website.

112. Excluded from the Classes are all judges and their staff assigned to this case and any members of their immediate families.

113. Plaintiff reserves the right to redefine the Classes and/or divide the Classes into subclasses at, or prior to, the class certification stage; in response to discovery; or pursuant to instruction by the Court.

114. This action is properly maintainable as a class action as specifically defined in Massachusetts Rule of Civil Procedure 23.

115. Numerosity: The Classes are so numerous that joinder of all class members is impracticable. Given the volume of Defendant's business, there are hundreds or thousands of Class members.

116. Commonality: This case presents common questions of law and fact, including but not limited to:

- a. Whether Defendant's practices relating to contemporaneous disclosures of Plaintiff's and Website User Class members' communications with Defendant to Meta and Google attached to PII and/or PHI violates G.L. c. 272, § 99;
- b. Whether Defendant's practices relating to the disclosures of Plaintiff's and the Patient Class members' communications with Defendants to Meta and Google attached to PII/PHI violates G.L. c. 214, § 1B;
- c. Whether an implied contract exists between Defendant and members of the Patient Class;
- d. Whether Defendant's alleged conduct breached the implied contract between Defendant and the Patient Class;
- e. Whether Defendant's practices relating to disclosures of Plaintiff's and Class members' communications with Defendant to Meta and Google were intentional;
- f. Whether Defendant's conduct harmed and continues to harm Plaintiff and Class members, and, if so, the extent of the injury;
- g. Whether and to what extent Plaintiff and Class members are entitled to damages and other monetary relief;
- h. Whether and to what extent Plaintiff and Class members are entitled to equitable relief; and

- i. Whether and to what extent Plaintiff and Class Members are entitled to attorneys' fees and costs.

117. Typicality: Plaintiff's claims are typical of the members of the Classes. Plaintiff and all members of the Classes visited the same website, programmed in the same way by Defendant, and had the same types of information sent to Meta and Google. Plaintiff and all members of the Patient Class are patients of Defendant.

118. Adequacy: Plaintiff will fairly and adequately protect the interests of the Classes because she and her experienced counsel are free of any conflicts of interest and are prepared to vigorously litigate this action on behalf of the Classes.

119. Questions of law and fact common to the Classes predominate over any questions affecting only individual members of the Classes, and a class action is superior to other available methods for the fair and efficient adjudication of this litigation. Defendant's conduct described in this Complaint stems from common and uniform policies and practices, resulting in common violations of the Wiretap Act, the Privacy Act, as well as Defendant's contractual and common law obligations. Members of the Class do not have an interest in pursuing separate actions against Defendant, as the amount of each Class member's individual claim is small compared to the expense and burden of individual prosecution. Class certification also will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning Defendant's practices. Moreover, management of this action as a class action will not present any likely difficulties. In the interests of justice and judicial efficiency, it would be desirable to concentrate the litigation of all Class members' claims in a single forum.

120. Defendant has acted or refused to act on grounds that apply generally to the Classes such that final injunctive relief is appropriate respecting the Classes as a whole.

121. In view of the complexities of the issues and the expenses of litigation, the separate claims of individual class members are insufficient in amount to support separate actions.

122. Yet, the amount which may be recovered by individual class members will be large enough in relation to the expense and effort of administering the action to justify a class action. The administration of this action can be handled by class counsel or a third-party administrator, and the costs of administration will represent only a small fraction of the ultimate recovery to be achieved.

COUNT I

INTERCEPTION OF WIRE COMMUNICATIONS IN VIOLATION OF G.L. c. 272, § 99 (Plaintiff Individually and on behalf of the Website User Class)

123. Plaintiff reiterates each of the allegations in the preceding paragraphs as if set forth at length herein.

124. G.L. c. 272, § 99 prohibits any person from willfully and secretly intercepting the contents of any wire communication through the use of any intercepting device unless given prior authority by all parties to a communication to do so.

125. Any person aggrieved by a violation of G.L. c. 272, § 99 “shall have a civil cause of action against any person who so intercepts, discloses, or uses such communications or who so violates her personal, property, or privacy interest.”

126. Defendant is a “person” under the statute.

127. All communications between Plaintiff or Class members and Defendant are “wire communications” under Massachusetts law because each communication is made using personal computing devices (*e.g.*, computers, smartphones, tables) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

128. An “interception” under the statute “means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire ... communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication[.]” G.L. c. 272, § 99B(4).

129. Defendant engaged and continues to engage in an “interception” by aiding Meta and Google to secretly record the contents of Plaintiff’s and Class members’ wire communications.

130. An “intercepting device” is “any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire ... communication[.]” G.L. c. 272, §99B(3) (setting forth exceptions that do not apply here).

131. The “intercepting devices” used in this case include the third-party source code utilized by Defendant which utilized (a) Plaintiff’s and Class members’ personal computing devices; (b) Plaintiff’s and Class members’ web-browsers; (c) Plaintiff’s and Class members’ browser-managed files; (d) Internet cookies; (e) Defendant’s own computer servers; and (f) the computer servers of Meta and Google.

132. Under the statute, “contents” is defined to mean “any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or the meaning of that communication.” G.L. c. 272, § 99B(5).

133. Defendant aided in and continues to aid in the interception of contents in that the data from the communications exchanged between Plaintiff or Class members and Defendant that were re-directed to and recorded by Meta and Google include information which identifies the parties to each communication, their existence, and their exact contents.

134. Under G.L. c. 272, § 99Q, aggrieved persons are “entitled to recover .. (1) actual damages but not less than liquidated damages computed at the rate of \$100 per day for each day

of violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation disbursements reasonably incurred.

135. In addition to statutory damages, Plaintiff and Class members were damaged by Defendant's violation in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private; and
- b. Defendants took valuable information from Plaintiff and Class members and derived benefit therefrom, including obtaining enhanced advertising and analytics services from Meta and Google, without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefits with Plaintiff or Class members.

COUNT II

INVASION OF PRIVACY IN VIOLATION OF G.L. c. 214, § 1B **(Plaintiff Individually and on behalf of the Patient Class)**

136. Plaintiff reiterates each of the allegations in the preceding paragraphs as if set forth at length herein.

137. G.L. c. 214, § 1B provides that "a person shall have a right against unreasonable, substantial, or serious interference with her privacy. The superior court shall have jurisdiction in equity to enforce such a right and in connection therewith to award damages."

138. All health care providers owe their patients a duty not to disclose medical information about the patient without the patient's informed consent.

139. G.L. c. 111, §70E provides that every patient of a Massachusetts health care facility shall have the right "to confidentiality of all records and communications to the extent provided by law."

140. The confidentiality of the patient-provider relationship is a cardinal rule of the medical profession which has come to be justifiably relied upon by patients seeking advice and treatments.

141. Plaintiff and members of the Patient Class are patients of Defendant.

142. Defendant owes Plaintiff and members of the Patient Class a duty of confidentiality.

143. Despite their duty not to disclose without informed consent, Defendant disclosed information relating to Plaintiff's and Patient Class members' medical treatment to Meta and Google without their knowledge or informed consent.

144. The information disclosed includes confidential medical information, including PHI such as Plaintiff's and Patient Class members' status as patients of Defendant, the contents of communications exchanged between Plaintiff or Patient Class members with Defendant, details regarding which doctors or support groups Plaintiff or Patient Class members scheduled appointments for, and information regarding medical diagnoses.

145. The disclosure of medical information with PII constitutes an unreasonable, substantial, and serious interference with Plaintiff's and Patient Class members' rights to privacy.

146. Plaintiff and Patient Class members were damaged by Defendant's violation in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Defendant took valuable information from Plaintiff and Class members and derived benefit therefrom, including obtaining enhanced advertising and analytics services from Meta and Google, without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefits with Plaintiff or Class members;

- c. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality. Plaintiff and Patient Class members would not have used Defendant's services, or would have paid substantially less for these services, had they known their medical information and PII would be disclosed.

COUNT III

BREACH OF IMPLIED CONTRACT

(Plaintiff Individually and on behalf of the Patient and Website User Classes)

147. Plaintiff reiterates each of the allegations in the preceding paragraphs as if set forth at length herein.

148. Plaintiff and Patient and Website Class members sought medical care and information from Defendant through the Baystate Website.

149. In order to obtain medical care and information from Defendant through the Baystate Website, Plaintiff and Patient and Website Class members provided their user data containing PII and private medical information to Defendant.

150. When Patient and Website Class members exchanged their PII and medical information in order to obtain information and services from Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their PII and medical information to third parties without their consent.

151. Plaintiff and Patient and Website Class members reasonably believed and expected that Defendant would not disclose their PII and medical information to third parties because, inter alia, Defendant made numerous promises not to disclose their information without consent and to not use their information for any purposes other than furthering the customer/patient relationship.

152. Plaintiff and Patient and Website Class members accepted Defendant's offers and provided their PII and medical information to Defendant in exchange for information and services.

153. Plaintiff and Patient and Website Class members would not have entrusted Defendant with their medical information and PII in the absence of an implied contract between them and Defendant obligating itself to not disclose Plaintiff's and Patient and Website Class members' medical information and PII without their consent.

154. Defendant breached these implied contracts by disclosing the medical information and PII of Plaintiff and Patient and Website Class members to third parties, *i.e.*, Facebook and/or Google, and using it for non-medical purposes, *i.e.*, to obtain enhanced marketing and analytical services.

155. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Patient and Website Class sustained damages as alleged herein, including:

- a. Sensitive and confidential information that Plaintiff and Patient and Website Class members intended to remain private is no longer private; and
- b. Defendant took valuable information from Plaintiff and Patient and Website Class members and derived benefit therefrom, including obtaining enhanced advertising and analytics services from Meta and Google, without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefits with Plaintiff or Class members.

156. Plaintiff and the Patient and Website User Class members are entitled to nominal, compensatory, and consequential damages as a result of Defendant's breaches of implied contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes, ask for judgment in their favor and that the Court award:

- a. Statutory damages of \$1,000 to Plaintiff and Website User Class members pursuant to G.L. c. 272, § 99Q;
- b. Damages for the violation of privacy as to Plaintiff and the members of Patient Class;
- c. Contract damages to Plaintiff and members of the Patient and Website User Classes for Defendant's breach of the implied contract;
- d. Punitive damages in an amount to be determined by a jury;
- e. Attorneys' fees and litigation costs reasonably expended;
- f. Appropriate injunctive relief enjoining the disclosures alleged herein which were made without Plaintiff's and Class members' express, informed written consent or other form of authorization;
- g. Granting such other and further relief, in law or equity, as this Court may deem appropriate and just.

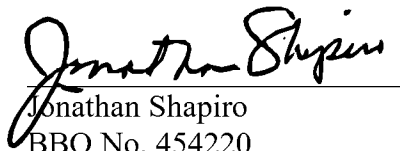
JURY DEMAND

Plaintiff, on behalf of herself and the Classes, demands a trial by jury on all issues triable by a jury.

Date: August 29, 2023

Respectfully submitted,

JANE DOE, INDIVIDUALLY AND ON BEHALF
OF ALL OTHER SIMILARLY SITUATED, By
Her Attorneys,


Jonathan Shapiro

BBO No. 454220

SHAPIRO & TEITELBAUM LLP

55 Union Street, 4th Floor

Boston, MA 02108

Tel.: (617) 742-5800

jshapiro@jsmtlegal.com

Sherrie R. Savett*
Lane L. Vines*
BERGER MONTAGUE PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel.: (215) 875-3000
ssavett@bm.net
lvines@bm.net

Sophia M. Rios*
BERGER MONTAGUE PC
401 B Street, Suite 2000
San Diego, CA 92101
Tel.: (619) 489-0300
srios@bm.net

* Pro hac vice motion to be filed

*Attorneys for Plaintiff
and the proposed Classes*

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT DEPARTMENT
CIVIL ACTION NO.: 2384CV01949

JANE DOE, INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY
SITUATED,

Plaintiff,

v.

BAYSTATE HEALTH SYSTEM INC.,

Defendant.

AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Jane Doe (“Plaintiff”), individually and on behalf of the class defined below, through their undersigned counsel, bring this Amended Class Action Complaint (“Complaint”) against Baystate Health System Inc. (“Baystate” or “Defendant”), and allege as follows.

1. This is a class action arising from Defendant’s systematic violation of the privacy rights of its patients by wiretapping the electronic communications of visitors to its website, <https://www.baystatehealth.org/> and <https://providers.baystatehealth.org/> (together, the “Baystate Website”), and violating patients’ rights to privacy with respect to their medical information.

2. During the relevant time period, Defendant’s Privacy Policy told patients that: “Baystate Health (BH) is committed to protecting your privacy and *we have taken steps to protect your information*. We have designed our website (baystatehealth.org) to allow you to visit most areas *without identifying yourself* or supplying personal information. For those areas where you are requested to provide identifiable information, we assure you that *it will only be used to support*

your customer/patient relationship with BH.”¹ Defendant further states that “[a]t Baystate Health, we understand that your medical information is personal, and we are committed to maintaining the privacy of this information.”²

3. Defendant, however, intentionally used various digital marketing tools on its website that were able to identify the patients on the Baystate Website, and purposefully and intentionally redirected to third parties Baystate patients’ personal health information, including those consumers’ individually identifiable health information (“IHII”) and protected health information (“PHI”) (referred to collectively as “Private Information”). Defendant’s use of these re-routing tools caused Baystate patients’ communications with Defendant and their Private Information to be automatically redirected to third parties in violation of patients’ reasonable expectations of privacy, and of both the express and implied promises of Defendant.

4. Specifically, at all relevant times, Defendant disclosed information about its patients’ communications—including their searches for medical information about conditions and procedures, the identities of their physicians, their requests to schedule appointments with physicians, registrations for support groups, patients’ request to log in to the patient portal, and when a patient clicks to make a telephone call in order to schedule an appointment with a specific doctor through the site—to Meta Platforms, Inc. (“Meta”) (formerly known as Facebook, Inc.) and/or Google without their knowledge, authorization, or consent.

5. Defendant’s conduct in disclosing patients’ Private Information to Meta and Google violates federal and Massachusetts law, including the federal wiretap act, known as the

¹ See <https://web.archive.org/web/20220622132503/https://www.baystatehealth.org/privacy-policy> (emphasis added).

² See <https://www.baystatehealth.org/notice-of-privacy-practices>.

Electronic Communications Privacy Act (“ECPA”) (18 U.S.C. § 2511(1) *et seq.*), and G.L. c. 111, § 70E (Patients’ and Residents’ Rights).

6. On behalf of herself and others similarly situated, Plaintiff seeks an order enjoining Defendant from further unauthorized disclosures of Plaintiff’s and Class members’ Private Information; awarding liquidated damages in the amount of \$10,000 per member of the Patient Class (defined below), contract and other damages as alleged, attorneys’ fees and costs; and granting any other equitable relief the Court deems appropriate.

PARTIES

7. Defendant Baystate Health, Inc. is a Massachusetts non-profit corporation with its principal offices at 759 Chestnut Street, Springfield, Massachusetts. Defendant touts that it is “a 716-bed independent academic medical center” and is “the community’s major referral hospital,” providing services that include: cancer care; critical care medicine; digestive disorder care; heart and vascular disease care; laboratory services; neurological disorders; obstetrics and gynecology care; and care for other injuries, illnesses, and conditions.³ Baystate designs and maintains, and/or directs the design and maintenance, of the Baystate Website from its offices in Massachusetts.

8. Plaintiff is an individual residing in Ludlow, Massachusetts. Plaintiff has visited the Baystate Website numerous times and has been treated by Defendant’s physicians.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over Defendant because it regularly conducts business throughout Massachusetts and has its principal place of business in Springfield. G.L. c. 223A, §§ 2 and 3.

³ See <https://www.baystatehealth.org/locations/baystate-medical-center>.

10. Venue is proper in Hampden County pursuant to G.L. c. 223, sec. 8(4) because Plaintiff resides in Hampden County and Defendant might sue or be sued in Hampden County. However, Plaintiff is seeking acceptance into the Business Litigation Session pursuant to Superior Court Administrative Directive 17-1 because this case is a consumer matter involving complex issues and cases based on similar claims have been assigned to the Business Litigation Session. *See Doe et al. v. Partners Healthcare System, Inc. et al.*, No. 1984CV01651, and *Doe v. Boston Medical Center Corporation*, No. 2384CV00326.

FACTUAL BACKGROUND

I. Massachusetts and Federal law protect personal privacy.

11. Under Mass. G.L. c. 214, § 1B, all persons “have a right against unreasonable, substantial, or serious interference” with their privacy.

12. Patient health information is specifically protected by the law. The prohibitions against disclosing patient personal health information include prohibitions against disclosing Private Information such as patient names, IP addresses, and other unique characteristics or codes. Massachusetts law subjects medical providers who treat conditions such as substance abuse to heightened duties of confidentiality. G.L. c 111B, § 11.

13. Moreover, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) requires covered entities, including Defendant, to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

14. These rules establish national standards for the protection of patient information, defined as IIHI which either “identifies the individual” or where there is a “reasonable basis to

believe the information can be used to identify the individual,” that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

15. HIPAA further limits the permissible uses and prohibits unauthorized disclosures of PHI.⁴

16. Federal law also protects persons from having the contents of their communications intercepted without their consent. Specifically, the ECPA, prohibits any person from willfully and secretly intercepting the contents of any wire communications through the use of any intercepting device unless given prior authority to do so.

17. As a health care provider, Defendant also has common law and statutory duties to protect the confidentiality of patient information and communications with individuals regarding its services.

II. Defendant promises patients that their electronic communications on the Baystate Website will be kept private.

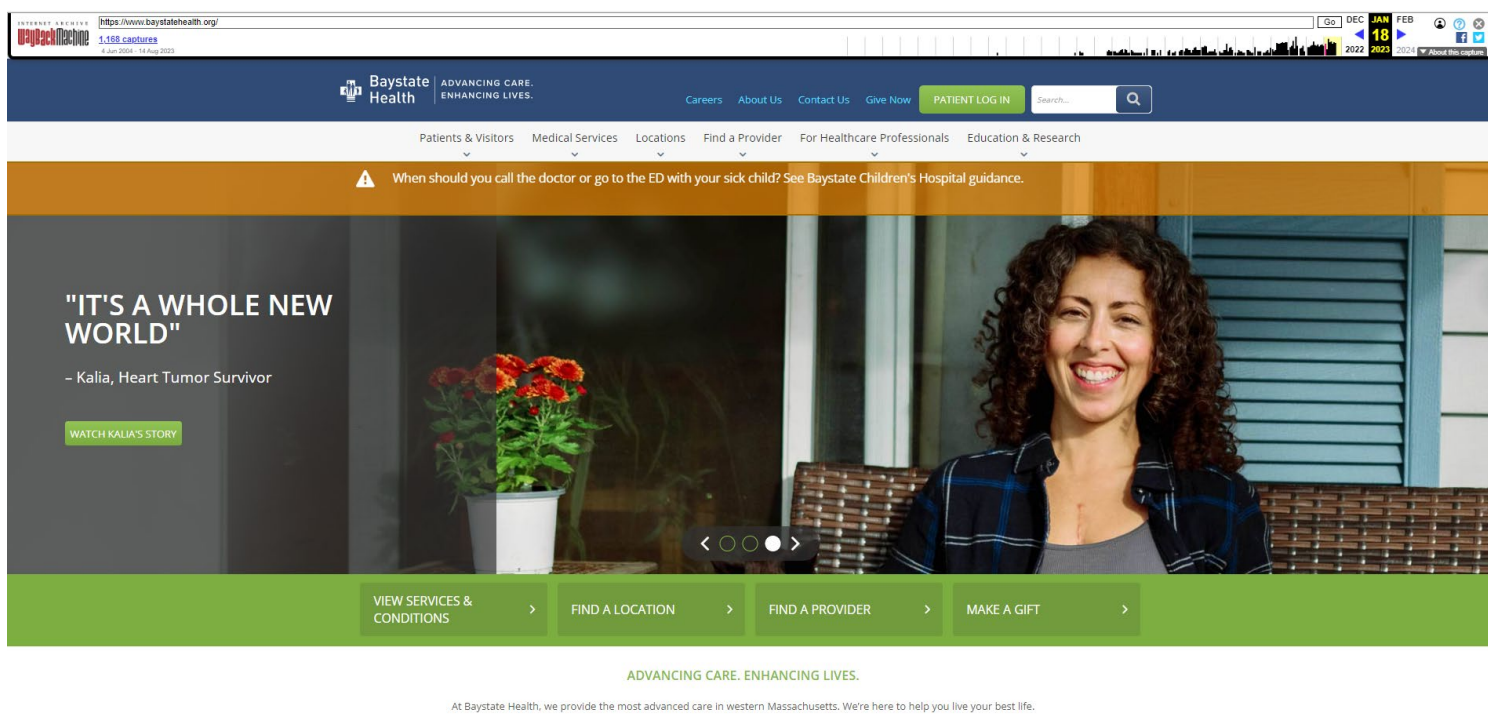
18. Defendant maintains the Baystate Website. The Baystate Website is designed for patients to communicate with Defendant, including by allowing individuals to research doctors and request to schedule appointments with doctors, register for support groups, research health conditions and learn about related services offered by Defendant, learn about medical procedures offered by Defendant, and sign in to a personal patient portal called MyBaystate. Patients can use search bars on Defendant’s website to type in the specific information, medical condition, medical procedure, type of doctor, or doctor that they want more information about.

19. According to Joel Vengco, Vice President of Information & Technology and Chief Information Officer for Baystate Health, in or about the beginning of 2015, Defendant’s website

⁴ 45 C.F.R. § 164.502.

added “My Baystate Health,” the online patient portal “that gives individuals access to portions of their medical records after they sign up.”⁵

20. Below is an example of the top of the Baystate Website homepage as it appeared on January 18, 2023.⁶ As depicted, the homepage provides patients with tools to sign into MyBaystate under the “Patient Log In” button, find a provider, explore medical services provided by Baystate and conditions that it treats, find a location, conduct a general search of the website, and more.



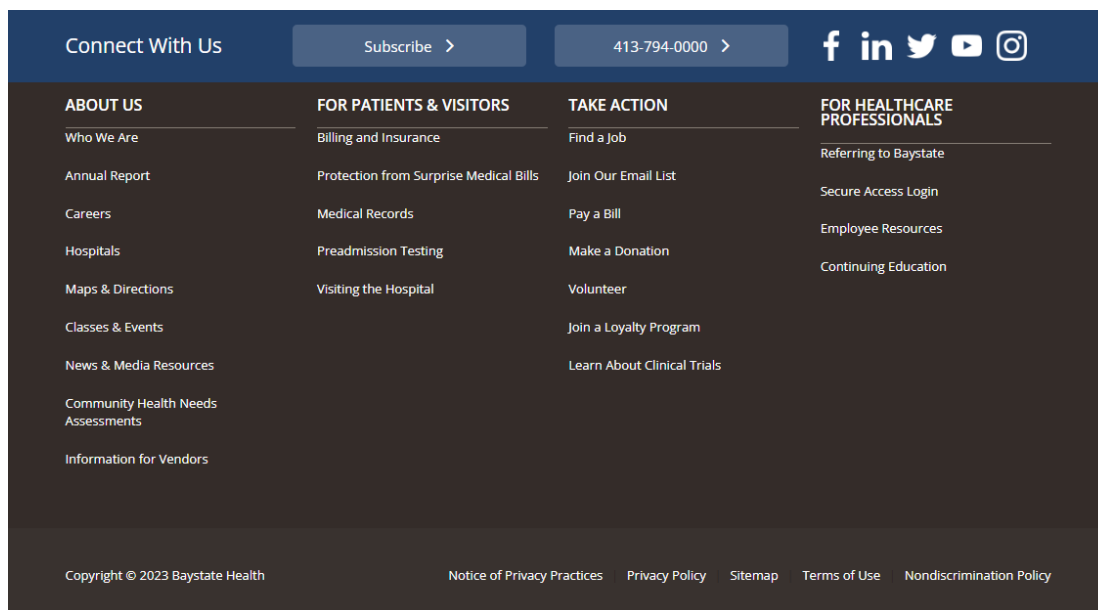
21. Defendant has statutory, regulatory, contractual, fiduciary, and common law duties to safeguard patients' Private Information from disclosure and ensure it remains private and confidential, and also expressly promises patients that Defendant will maintain the confidentiality

⁵ See <https://healthcarenews.com/think-tank-techspring-center-brings-silicon-valley-model-to-springfield/>.

⁶ See <https://web.archive.org/web/20221223120755/https://www.baystatehealth.org/>.

of patient information and communications and will use that information ***“only for your customer/patient relationship with Baystate Health.”***

22. As displayed at the bottom of its homepage, Defendant provides patients and website visitors links to access Defendant’s Notice of Privacy Practices and Privacy Policy.



23. As shown above, Defendant’s Privacy Policy is located at the bottom of the Baystate Website in small font among several other links. Before it was last updated on May 15, 2023, Defendant stated in its Privacy Policy that ***“Baystate Health (BH) is committed to protecting your privacy. We have designed our website (baystatehealth.org) to allow you to visit most areas without identifying yourself or supplying personal information.”***⁷ Defendant went on to promise that ***“We do not disclose your personal information unless the following conditions are met: · You provide to us a specific written consent, or · We are required by law.”***⁸ Defendant also misleadingly stated that ***“If you are browsing the BH web site, a cookie identifies only your browser!”***⁹ As explained below, these promises of confidentiality and anonymity were illusory.

⁷ <https://web.archive.org/web/20220622132503/https://www.baystatehealth.org/privacy-policy>.

⁸ *Id.*

⁹ *Id.*

24. Defendant's Notice of Privacy Practices is also located at the bottom of the Baystate Website. In it, Defendant states *"At Baystate Health, we understand that your medical information is personal, and we are committed to maintaining the privacy of this information,"* and links to the HIPAA Notice of Privacy Practices in both English and Spanish. HIPAA, short for the Health Insurance Portability and Accountability Act, is a federal law that establishes national standards to protect individuals' medical records and other individually identifiable health information.

25. The HIPAA Notice is a two-page document entitled "Baystate Health Notice of Privacy Practices – Your Information. Your Rights. Our Responsibilities" (effective March 1, 2021).¹⁰ Those Privacy Practices explain:

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. If you have questions about this notice, please contact the Baystate Health Privacy Office at (413) 794-7955 or complianceoffice@baystatehealth.org. This notice describes the privacy practices of Baystate Health, Inc. ("Baystate") and its affiliated entities.

Those Privacy Practices also provide numerous assurances for the privacy of information and Baystate's responsibilities, including the following statements:

YOUR CHOICES:

For certain health information, you can tell us your choices about what we share. ...

If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety. In these cases we never share your information unless you give us written permission:

- Marketing purposes

¹⁰ See <https://www.baystatehealth.org/-/media/files/about-us/corporate-information/hipaa-notice-of-privacy-practice-english.pdf?la=en>.

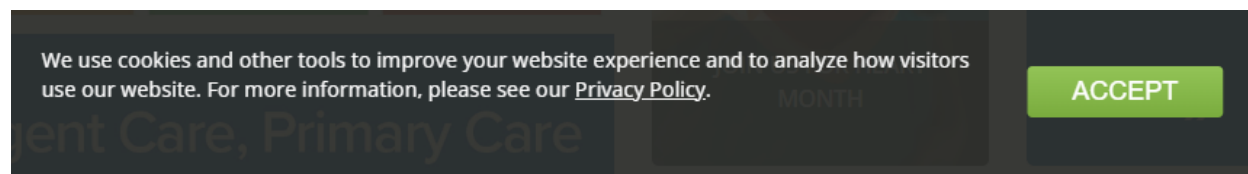
- Sale of your information

OUR RESPONSIBILITIES

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing.

26. These repeated promises by Defendant inform patients that they can use Defendant's website anonymously and that Defendant will not disclose Private Information and other sensitive information to third parties.

27. Moreover, before January 2023, Defendant's Website did not feature any notification to patients that cookies were used on the website. At some point in January 2023, Defendant began prompting patients with the following "pop up" notification at the bottom of its homepage. There was no such warning and no prompt to "accept" the use of cookies on the Baystate Website before January 2023.



28. As described above, the Privacy Policy in January 2023 did not disclose to patients that their communications on the website would be shared, along with Private Information, with third parties. The pop-up notification was therefore insufficient to obtain patients' consent to disclose their communications and Private Information to third parties.

III. Defendant systematically violates its patients' privacy rights.

29. Despite these express promises and its legal duties, Defendant chose to share the content of its patients' communications with Meta and Google by intentionally installing tracking technology on the Baystate Website. Defendant disclosed the communications to Meta and Google without the knowledge or consent of patients.

A. Defendant's Use of the Meta Pixel.

30. The Meta Pixel is a snippet of code, invisible to patients as they view a website, that tracks users as they navigate the web, logging which pages they visit, which buttons they click, and certain information they enter into forms or search requests.

31. Defendant began using the Meta Pixel by at least January 1, 2021. The presence of the Meta Pixel on Defendant's website can be shown using the Wayback Machine,¹¹ as shown in the image below reflecting the code that Defendant installed on its website to enable the Meta Pixel on January 1, 2021.¹²

```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://web.archive.org/web/20210101101705/https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '247095132483787');
  fbq('track', 'PageView');
</script>
<noscript>
   "
</noscript>
<!-- End Facebook Pixel Code -->
..
```

¹¹ The Wayback Machine is a digital archive of the World Wide Web founded by the Internet Archive, a nonprofit based in San Francisco, California. Created in 1996 and launched to the public in 2001, it allows the user to go “back in time” and see how websites looked in the past.

¹² See <https://web.archive.org/web/20210101101705/https://www.baystatehealth.org/>.

32. Discovery will show that Defendant programmed the Meta Pixel to send information to Facebook about all website visitors—including Facebook users and non-Facebook users.

33. The Meta Pixel sends information to Facebook via scripts running in a person's internet browser, so each data packet comes labeled with an IP address that can be used by Facebook in combination with other data to identify an individual or household.

34. An IP address is a number that identifies a specific device connected to the Internet and reveals geolocation. Under HIPAA, an IP address is considered PHI (45 C.F.R. § 164.514(b)(2)(i)(0)).

35. If a patient is logged into Facebook when they visit a website that has installed the Meta Pixel, the communications can also be linked to a specific Facebook account which identifies a Facebook user's name, photo, and profile.

36. Facebook has over 2.9 billion active monthly users.¹³ Facebook's Community Standards require users to use their real identities when signing up on the platform. This means users are only allowed one account and must use the name they use in "everyday life,"¹⁴ including first and last name.¹⁵ Users must also provide their birthday and gender.

37. When a user logs into Facebook using an internet browser, such as Google Chrome or Microsoft Edge, Facebook places several cookies on the user's browser.

¹³ See <https://www.reuters.com/technology/facebook-owner-meta-forecasts-q1-revenue-below-estimates-2022-02-02/>.

¹⁴ See https://transparency.fb.com/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fintegrity_authenticity.

¹⁵ See <https://www.facebook.com/help/229715077154790/>.

38. A cookie is a piece of code placed on a browser by a server that contains information. A cookie can store different types of information, but the basic premise is to identify a) you and b) the website you visited that placed the cookie to begin with.

39. One of the cookies placed by Facebook on a user's browser upon login is the "c_user" cookie which contains the user's Facebook ID number. This cookie remains on a user's browser as long as they do not hit "Log Out" when they leave Facebook. Even if the person never visits Facebook.com using that browser again, the cookie will remain on the device for one year since the last visit to Facebook.

40. The long life of the c_user cookie is intentional—not only does the cookie allow Meta to identify users when they visit Facebook.com, it also allows Meta to track the user's activity across the web on the same browser. Because the Facebook ID is specific to a person, Meta can also match up a user's activity across devices using different browsers if that user has also logged in on another device.¹⁶

41. Website owners can also set additional Meta cookies, such as the "fr" or "_fbp" cookies and others, that unlike the c_user cookie, collect information on all patient—not just logged in Facebook users. Like the c_user cookie, these additional Meta cookies appear to contain unique identification numbers that are disclosed to Facebook along with the information tracked by the Meta Pixel, thereby permitting Facebook to target patients with personalized ads across different websites even if they are not Facebook users.

42. By tracking a specific person's movements across the web and across devices, Facebook collects enormous amounts of data regarding patients' interests, behavior, and

¹⁶ See <https://www.facebook.com/business/news/cross-device-measurement>.

connections.¹⁷ The quantity and quality of this data allows Meta to generate billions in advertising revenue—allowing businesses to target people with specific interests, target advertisements to specific people who visited their site but did not complete a purchase, and analyze the types of people that are visiting their site by leveraging user demographics, interests, and behaviors on other websites.

43. Businesses—like Defendant—access these services from Meta in part by installing the Meta Pixel on their website.

44. Pixels, also known as “web beacons,” are often small transparent images that an internet browser downloads like any other image on a website. When you visit a web page which contains the Meta Pixel, the pixel essentially contacts the Facebook ad server.

45. The business installing the pixel can program the pixel to record specific acts and communications, such as when a user places an item in their shopping cart, clicks a certain button, types in a search into a search bar, or otherwise interacts with the website.¹⁸ Meta receives the event information along with personal identifying information contained in the cookies described above.

46. The disclosures to Meta occur contemporaneously with communications between the website user and the website. The code causes the communications to be recorded on the user’s device and then transmitted in a package to Meta. By design, Meta receives the exact contents of the communications before the full response from the website has been rendered on the website users’ screen and while the communication between the website and the website user is ongoing.

¹⁷ See <https://www.facebook.com/business/ads/ad-targeting>.

¹⁸ See <https://developers.facebook.com/docs/meta-pixel/advanced>.

47. If a business does not install the Meta Pixel, information on a user's actions on the website would not be communicated to Meta.

48. Once the information is in the possession of Meta, Meta uses it for advertising and analytics purposes. Businesses know that Meta can identify the Facebook users visiting their website and track people who are not Facebook users across websites. The value for the business in programming their website with the pixel is derived from Meta's ability to identify the website visitors, track their behavior on their website, and link them to Meta data on their interests, behaviors, and connections, and to allow the business to target advertisements to specific users.

49. In some cases, a Facebook user can confirm that a website has shared information about their visit to that website with Meta via the Meta Pixel on a certain date by reviewing their "Off-Facebook Activity." Off-Facebook activity is "a summary of activity that businesses and organizations share with [Facebook] about [a user's] interactions, such as visiting their apps or websites."¹⁹ The Off-Facebook Activity report provided by Facebook to users, however, is an incomplete report of all activity on non-Facebook sites that has been shared with Meta by third parties such as Defendant.

50. On June 16, 2022, an article was published on The Markup titled "Facebook Is Receiving Sensitive Medical Information from Hospital Websites."²⁰ The Markup is a nonprofit newsroom that investigates and publishes stories regarding technology. The article detailed how hospitals using the Meta Pixel were allowing the tracking tool to collect patients' sensitive health information, including details about their medical conditions, prescriptions, and doctor's appointments, along with users' IP addresses. As detailed by the article, several hospitals removed

¹⁹ See <https://www.facebook.com/help/2207256696182627>.

²⁰ See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.

the Meta Pixel from the most sensitive parts of their websites, such as pages used to book appointments, or removed the Meta Pixel altogether after the article highlighted the privacy violations occurring.

51. After the Markup article was published, and as more and more lawsuits were filed against hospitals and healthcare providers for privacy violations related to the Meta Pixel, Defendant likely recognized the privacy violations on its own website. Thus, as evidenced by the disappearance of the Meta Pixel code as viewable on the Wayback Machine, Defendant removed the Meta Pixel from its website by April 2023. Defendant also added the cookie pop up notification to its website in January 2023 and modified its Privacy Policy in May 2023 to add additional disclosures regarding the use of cookies.

B. Defendant's Use of Google Analytics.

52. Defendant began using Google Analytics by at least January 1, 2021. The presence of the Google Analytics code and other Google code can be shown using the Wayback Machine, as in the image below reflecting the code Defendant installed on its website to enable transmissions to Google from Defendant's website.

```
<!-- Google Tag Manager -->
<noscript>
  "<iframe src="//web.archive.org/web/20210101101705if_/https://www.googletagmanager.com/ns.html?
  id=GTM-W98BKP" height="0" width="0" style="display:none;visibility:hidden"></iframe>"
</noscript>
<script>
  (function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
  new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
  j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
  '//web.archive.org/web/20210101101705/https://www.googletagmanager.com/gtm.js?
  id='+i+dl;f.parentNode.insertBefore(j,f);
  })(window,document,'script','dataLayer','GTM-W98BKP');
</script>
<!-- End Google Tag Manager -->
```

53. Defendant also installed Google Analytics code on <https://providers.baystatehealth.org/>, the part of its website where patients can search for doctors and request appointments with specific doctors.

54. Defendant sends patient information to Google using Google Analytics, a web analytics service, which allows website owners to track visitor actions on their website and measure the effectiveness of advertising. Specifically, Defendant uses technology such as Google tag manager and cookies to send the contents of patients' communications with the Baystate Website and IP addresses to Google.

55. Google Analytics automatically collects IP addresses of individual Internet users in order to facilitate and track Internet communications. However, Google Analytics offers website owners an opt-in IP anonymization feature. According to Google, this feature is designed to help site owners comply with their own privacy policies and the recommendations of data protection authorities. If the IP anonymization feature is enabled by the website owner, an additional parameter is added to the communications between website visitors' computers and the Google Analytics server, defined as `aip=1`. Accordingly, when the "aip" parameter does not appear, the IP address is not anonymized, enabling Google to identify a website user's IP address connected with their communications made via the website.

56. Baystate did not opt-in to Google Analytics' IP anonymization feature, as evidenced by the absence of the `aip=1` parameter on communications sent to Google from the Baystate Website.

57. Simply put, Defendant intentionally programmed Google Analytics in such a way as to disclose the content of patients' communications with the Baystate Website along with patients' Private Information in the form of IP addresses.

58. Even after Defendant removed the Google code from <https://providers.baystatehealth.org/>, Defendant continued to use Google Analytics on <https://www.baystatehealth.org/> and to share patients' sensitive communications on that website with Google.

C. The Nature of Defendant's Intentional, Unauthorized, Unnecessary, and Unlawful Disclosures.

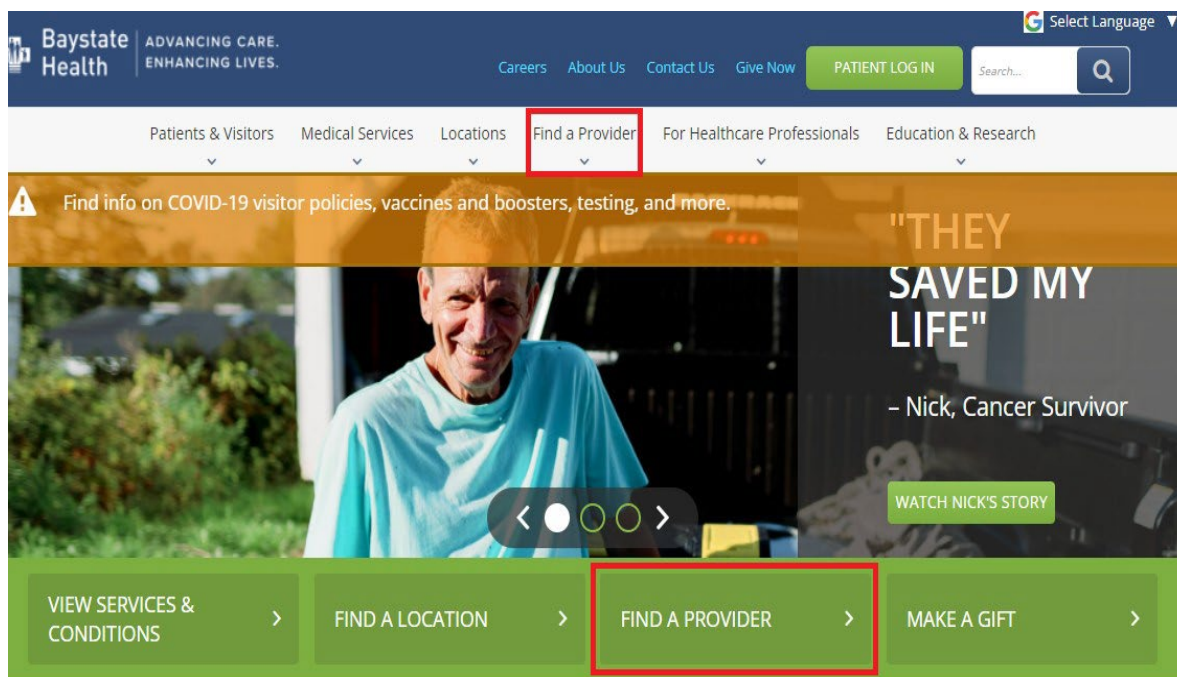
59. As intentionally implemented by Defendant, the Meta Pixel and Google Analytics tag causes Private Information, as well as the exact contents of the communications exchanged between Defendant and its patients, to be sent to Meta and Google.

60. Defendant's third-party disclosures occur contemporaneously with communications by Plaintiff and Class members to Defendant's website.

61. By design, Meta and Google receive and record the exact contents of these communications before the full response from Defendant to Plaintiff or a Class member has been rendered on the screen of the patients' devices and while the communications between Defendant and patients remains ongoing.

62. Defendant installed the Google and Meta code on its website in a way that enabled transmissions from across Defendant's website, not just the web pages detailed herein. Discovery will show the full scope of Defendant's disclosures to Meta and Google. The examples provided below are for illustrative purposes only and do not attempt to describe the full scope of Defendant's privacy and wiretap violations.

63. When a patient clicks on the “Find a Provider” links provided by Defendant on the home page, they are directed to <https://providers.baystatehealth.org/>, where Defendant installed the Google tracking technology.



64. At this website, patients can navigate to a page providing a list of doctors and where they are able to search for a doctor by name, condition, specialty, location, gender, language, and more.

What do you need help with today?

Enter a Condition, Specialty, or Provider Name 🔍

COVID-19: Learn about the vaccine, testing, visitor restrictions & more. If you are experiencing a medical emergency, please call 9-1-1. ×

Distance Reset

Within 25 miles ▼

City, State or ZIP 🔍

Use current location

Specialties

Choose Specialty ▼

Locations


Type here... ▼

Online Scheduling

☐ 📅 Book Online (101)

1953 providers found Best Match | Availability | A-Z | Z-A

Video Visit



Pamela Jean Behrens, CNP

VIRTUAL VISITS AVAILABLE

★★★★★ 4.8 out of 5 (87 ratings)

Specialties
Urogynecology

Affiliations
Baystate Medical Center

Schedule Appointment

🕒 Available within 3 days*

📺 Video Visit

📞 Phone Visit


A member of Baystate Medical Practices

Practice Locations

Baystate Urogynecology
Tolosky Center, 3300 Main Street, Suite 4B, Springfield, MA 01199 (Map)

Phone
413-795-8764

Video Visit



Catherine Henry Tipton, CNP

ACCEPTING NEW PATIENTS VIRTUAL VISITS AVAILABLE

★★★★★ 4.9 out of 5 (62 ratings)

Specialties
Surgical Oncology

Affiliations
Baystate Medical Center
Baystate Noble Hospital

Schedule Appointment

🕒 Available within 3 days*

📺 Video Visit

📞 Phone Visit

A member of Baystate Medical Practices

65. As shown in the image to the right, patients can enter the parameters they would like to use to search for a doctor. When a patient entered the parameters, Defendant disclosed the parameters and search terms used by patients to Google.

66. After a patient conducts a search for a provider, Defendant displays a list of doctors that meet the search criteria, such as the list shown below.

Distance

Within 25 miles ▼

Springfield, MA, USA 🔍

Use current location

Specialties

× Infectious Diseases ▼

Baystate Medical Practice Provider

☒ Show only (2)

Affiliations

☒ Baystate Franklin Medical Center (2)

☐ Baystate Medical Center (2)

☐ Baystate Noble Hospital (2)

☐ Baystate Wing Hospital (1)

Age Groups Seen

☒ Adults (2)

Accepting New Patients

☒ Yes (2)



Provider Gender

☒ Female (2)

Language

☒ English (2)

3 providers found near Springfield, MA 01199, USA [Clear Filters](#) [Best Match](#) | [Availability](#) | [Distance](#) | [A-Z](#) | [Z-A](#)

Megan C. Gallagher, MD

ACCEPTING NEW PATIENTS


VIRTUAL VISITS AVAILABLE


Specialties
Infectious Diseases

Affiliations
Baystate Franklin Medical Center
Baystate Medical Center
Baystate Noble Hospital
Baystate Wing Hospital



A member of
Baystate Medical Practices

Schedule Appointment

 Video Visit

 Phone Visit

Practice Locations	Phone	Distance
Baystate Infectious Disease 759 Chestnut Street, Springfield, MA 01199 (Directions)	413-794-7394	0.08 miles
Baystate Infectious Disease Tolosky Center, 3300 Main Street, Suite 3C, Springfield, MA 01107 (Directions)	413-794-7394	0.21 miles

Claire E. Magauran, MD

ACCEPTING NEW PATIENTS


VIRTUAL VISITS AVAILABLE


Specialties
Infectious Diseases:
 ◦ HIV Medicine

Affiliations
Baystate Franklin Medical Center
Baystate Medical Center
Baystate Noble Hospital

A member of
Baystate Medical Practices

Schedule Appointment


 Video Visit

 Phone Visit

Practice Locations	Phone	Distance
Baystate Infectious Disease 759 Chestnut Street, Springfield, MA 01199 (Directions)	413-794-7394	0.08 miles

67. Patients can then select a doctor that they are interested in. Once patients select a doctor, Defendant also sent this information to Google.

[Return to search results](#) or [Start a new search](#)



Megan C. Gallagher, MD
Infectious Diseases

ACCEPTING NEW PATIENTS

VIRTUAL VISITS AVAILABLE

Schedule Appointment

[About](#) | [Expertise](#) | [Insurance](#) | [Schedule Appointment](#)

About Megan C. Gallagher

Provider Gender	Female
Language	English
Age Groups Seen	Adults
Practice Groups	Baystate Infectious Disease

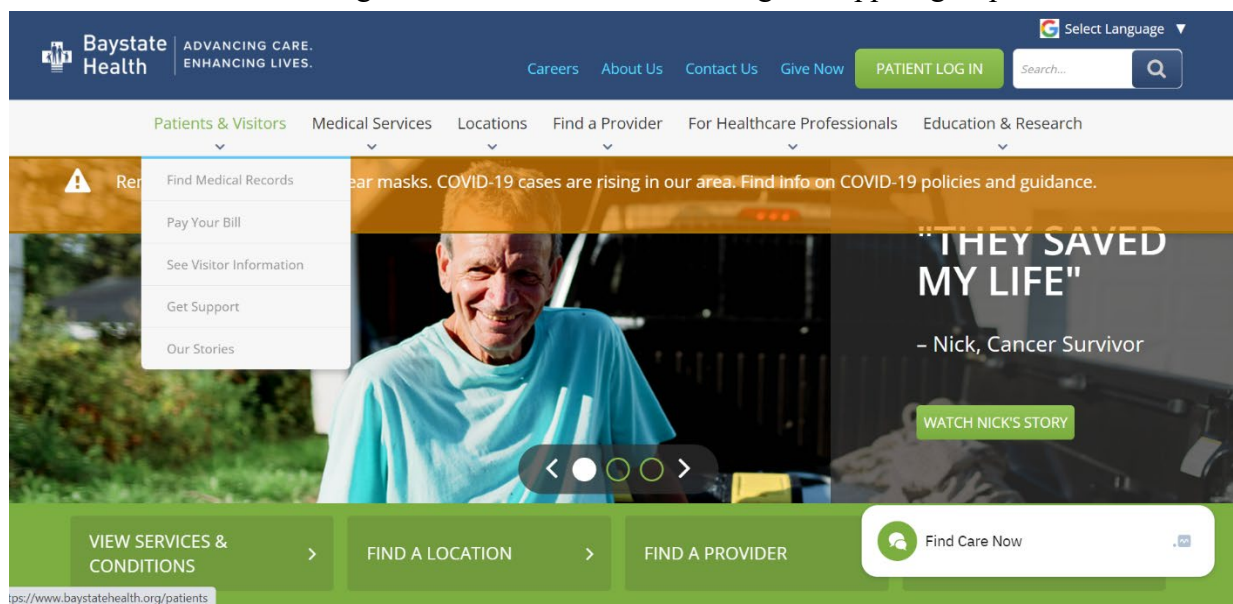
68. For example, as shown below, when a patient searches for a female doctor who specializes in infectious diseases for adults and accepts patients in Springfield, specifically in

Request URL: https://www.google-analytics.com/collect?v=1&v=j96&a=503589314&t=timing&s=2&d1=https%3A%2F%2Fproviders.baystatehealth.org%2Fprovider%2FMegan%2BC.%28Gallagher%2F759071%3Fdissplay_location%3D%25C%2520VA%25C%2520USA%25C%2520distance%3D00%26filter%3Dspecialties.specialty.untouched%253Infectious%2520Diseases%26filter%3Dnetwork_affiliation.s.name%253Baystate%2520Franklin%2520Medical%2520Center%26filter%3Dage_groups_seen.name%253Adults%26filter%3Dgender%253Female%26filter%3DLanguages.language%253English%26location%3D38.7892801%252C-77.1872035999999999%26from%3Dsearch-list&l=he-il&de=UTF-8&dt=Dr.%20Megan%20C.%20Gallagher%2C%20MD%20-%20Springfield%2C%20MA%20-%20Infectious%20Diseases%20-%20Schedule%20Appointment&sd=24-bit&sr=1920x1080&vp=1472x961&je=0&lp=3883&pt=380&ds=2078&r=38rtp=965&tcp=403&id=2622&c1t=2622&gst=1625&b=1702&cst=1626&u=SDCACEABBAAAAC&-tid=&gid=&cid=14244047393.1654590285&did=UA-9927205-1&_gl_id=498425997.165459028>ag=2wg660P80Wl8F&z=121258638

71. For example, as shown below, when a patient clicks the “Schedule Appointment” button, Defendant disclosed to Google that the patient was scheduling an appointment with a specific doctor, the search that led the patient to that specific doctor, and again the patient’s IP address.

21

72. On <https://www.baystatehealth.org/>, Defendant offers patients the option to participate in various support groups. Patients are able to click the "Patients & Visitors" button on the main page and choose "Get Support", or search for a specific event through the search bar. Support groups offered include, for example, a virtual weight loss surgery support group which is open to patients enrolled in Baystate Health's bariatric surgery program, cancer support groups which are open to those who have been diagnosed with cancer, breast cancer support groups open to those who have been diagnosed with breast cancer, and grief support groups.



73. Information relating to past, present, or future physical or mental health or condition of an individual including specific diagnoses, is PHI under HIPAA.

74. Defendant's website allows patients the ability to register for support groups on the website.

JOURNEY THROUGH GRIEF SUPPORT GROUP

Please join us for a weekly bereavement support group

JOURNEY THROUGH GRIEF

Journey Through Grief is a weekly bereavement support group for adults who are struggling with the loss of a loved one. Registration is required. The group is free of charge.

This educational support group will provide materials and information on the grieving process, so as to better understand the grief experience and gather tools to cope with loss.

Wednesdays, 10- 11 am

January 16 - March 5, 2019

330 Main St, 4th Floor, Room # 489

Springfield, MA

To register please call or email, Betsy Flores, Bereavement Coordinator, [Baystate Hospice](mailto:betsy.flores@baystatehealth.org) at 413-794-6559 or betsy.flores@baystatehealth.org



75. However, when a patient clicks the “Register” button, Defendant sends this information to Meta and Google along with the patients’ IP address and identifying Facebook cookies.

```
Request URL: https://www.google-analytics.com/collect?v=1&_v=j96&a=1184011751&t=event&ni=0&s=1&dl=https%3A%2F%2Fwww.baystatehealth.org%2Fabout-us%2Fcalendar%2Fspiritual-services%2Fjourney-through-grief&ul=en-us&de=UTF-8&dt=Journey%20Through%20Grief%207C%20Baystate%20Health&sd=24-bit&sr=1920x1080&vp=1196x961&je=0&ec=mailto&ea=REGISTER&l=https%3A%2F%2Fwww.baystatehealth.org%2Fabout-us%2Fcalendar%2Fspiritual-services%2Fjourney-through-grief&u=SCCAiEAB8~&jid=&gjid=&cid=1332328207.1649685651&tid=UA-9927205-1&_gid=126151795.1651479903&gtm=2wg4r0W988KP&cg1=Service%20Line&z=1082919632
```

76. Defendant also allows patients to request specific information by submitting requests in the search bar provided at the top of the home page. Patients can search for doctors, information about conditions that Baystate Health treats, treatment options, and more.

77. Defendant disclosed to Meta and Google the text of the searches typed into the search bar by patients, along with their IP addresses and Private Information.

78. As also shown in the images above, next to the search bar on the home page, Defendant provided a green “PATIENT LOG IN” button to patients. This button directs patients to <https://mybaystate.baystatehealth.org/#/login>, where they can log in to the patient portal and access medical records, make payments, view appointments and make appointments, and more. The button was provided by Defendant throughout the Baystate Website and other links to the

patient portal were provided to patients as well, such as on the medical records page:

<https://www.baystatehealth.org/patients/medical-records>.

79. The fact that a person is a patient of a medical provider is PHI under HIPAA.

80. When a patient clicked this button or the other links provided to the MyBaystate portal login page, Defendant programmed its website to disclose to Google the information highlighted below, which contains the fact that the patient was requesting to log in to the patient portal, along with personally identifiable data such as their IP address. The code shown below is visible using the WayBack Machine to interact with the page as it was during the relevant time

```
https://web.archive.org/web/20190801140235/https://www.google-analytics.com/r/collect?v=1&_v=j77&
a=789417493&t=event&ni=0&_s=1&dl=https%3A%2F%2Fwww.baystatehealth.org%2Fpatients%2Fmedi
cal-records&ul=en-us&de=UTF-8&dt=Medical%20Records%20%7C%20Baystate%20Health&sd=24-bit&
sr=1920x1080&vp=1718x1034&je=0&fl=32.0%20r0&ec=Outbound&ea=Click&el=https%3A%2F%2Fmy
baystate.baystatehealth.org%2F%3F_ga%3D2.222881438.460604823.1657167446-1194375229.165716744
6%23%2Flogin&_u=aGDACEABB~&jid=154672583&gjid=249462703&cid=1194375229.1657167446&tid
=UA-9927205-1&_gid=460604823.1657167446&r=1&gtm=2wg7o0W98BKP&z=105919696
```

period:

81. These third-party disclosures were made by Defendant without the patients' knowledge, consent, or any affirmative action taken. As described above, Defendant does not provide any information to patients that would alert them to the fact that the contents of their communications on the Baystate Website are disclosed to Meta and Google. In fact, Defendant misled patients to believe that they can use the website confidentially.

IV. Defendant chose to intercept and then disclose patients' Private Information to enrich itself.

82. Defendant is not required to make disclosures to Meta or Google in the ordinary course of business. The Baystate Website and services can function without the code that Defendant installed on the Baystate Website to enable the disclosures, as evidenced by Defendant's removal of the tracking code from many places on the website. For example, the

disclosures are not necessary for Defendant to maintain a website or use social media marketing tools.

83. It is possible for Defendant to allow patients to search for information about their health conditions and find doctors without disclosing those searches to third parties. It is also possible for Defendant to allow patients to schedule appointments with providers and register for support groups without disclosing those communications to third parties.

84. Despite these facts, Defendant affirmatively chose to provide Meta and Google secret and invisible “windows” that allowed them to intercept and then record the exact contents of patient communications on the Baystate Website and Private Information.

85. Defendant chose to install the tracking technology on the Baystate Website for marketing and/or analytics purposes. In exchange for Private Information about Defendant’s patients, Meta and Google use the information to provide enhanced online advertising services and/or analytical services to Defendant.

86. Further, once the information is shared by Defendant with Meta and Google, Defendant loses the ability to further control the dissemination and use of the Private Information and the disclosed communications. Discovery will show that Meta and Google use the information disclosed by Defendant for their own purposes.

87. The monetization of the data disclosed by Defendant, both for its own purposes and those of the third parties, demonstrates the inherent value of the information collected.

88. By sending this sensitive information and communications to third parties, Defendant violates Plaintiff’s and Class members’ rights to privacy in that information and communications and their right not to have their Private Information shared without their knowledge or consent.

FEDERAL REGULATORY WARNINGS

89. On July 20, 2023, the Federal Trade Commission (“FTC”) and the U.S. Department of Health and Human Services’ (“HHS”) Office for Civil Rights (“OCR”) issued a press release explicitly cautioning hospitals and telehealth providers, such as Baystate, about “the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers’ sensitive personal health data to third parties.”²¹

90. In that press release, Samuel Levine, Director of the FTC’s Bureau of Consumer Protection admonished that:

When consumers visit a hospital’s website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers’ health information from potential misuse and exploitation.

91. The press release further advised that HHS and the FTC had “sent the joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user’s online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.”

92. In their letter to healthcare providers dated July 20, 2023, HHS and the FTC “reiterated the risks posed by the unauthorized disclosure of an individual’s personal health

²¹ See <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.” *Id.*²²

93. Indeed, as reported, “HHS highlighted these concerns in a bulletin it issued late last year that reminded entities covered by the Health Insurance Portability and Accountability Act (HIPAA) of their responsibilities to protect health data from unauthorized disclosure under the law.” Those admonitions even extended to companies not covered by HIPAA as providers “still have a responsibility to protect against the unauthorized disclosure of personal health information—even when a third party developed their website or mobile app. Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC’s Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC’s Health Breach Notification Rule.”

94. Earlier this year, in a March 16, 2023, the FTC Office of Technology issued a blog posting titled “Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking,” in which the FTC provided further cautionary warnings to about the use of pixel tracking, such as the Meta Pixel, and the serious privacy violations such tracking causes.²³ In that blog, the FTC discussed its recent

²² A copy of the letter dated July 20, 2023, that was signed by the Director of HHS’s Office for Civil Rights, Melanie Fontes Rainer, and the Director of the FTC’s Bureau of Consumer Protection is available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

²³ See <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>.

enforcement actions against GoodRx and BetterHelp, two digital healthcare platforms, for allegedly sharing user health data with third parties for advertising.

PLAINTIFF'S EXPERIENCE

95. Plaintiff Jane Doe has and had objectively reasonable expectations of privacy in communications with the Baystate Website that are grounded in her status as a patient of Defendant's, Defendant's legal obligations to maintain the confidentiality of wire communications and communications with patients, state and federal laws protecting the confidentiality of patient communications and medical information, and Defendant's express promises, as described above.

96. Plaintiff has been a patient of Defendant's for at least 10 years and is a current patient. Plaintiff regularly exchanged communications with Defendant on the Baystate Website during the relevant time period.

97. In the last few years, Plaintiff has communicated on the Website to obtain information related to breast cancer screenings and schedule a mammogram, to log in to the MyBaystate patient portal, and to search for providers.

98. Defendant disclosed Plaintiff's confidential communications with Defendant through the Baystate Website to Meta and Google.

99. Plaintiff has confirmed that Defendant disclosed her communications and sensitive information to Meta through the Off Facebook Activity Report. Plaintiff has been a Facebook user since at least 2010. Even though such reports provided by Facebook are incomplete, a report generated by Plaintiff captured approximately **80 disclosures** of Plaintiff's communications by Defendant to Meta between November 19, 2021 through April 10, 2023.

100. The presence of this data on the report confirms that the c_user cookie was present on Plaintiff's device and operating as Defendant intended when it installed it on the Baystate Website during the relevant time period.

101. Google cookies were also present on the device Plaintiff used to visit Defendant's website.

102. The demonstrated operation of the Facebook cookies on Plaintiff's device also indicates that the Google cookies supporting the Google tracking code installed by Defendant on the Baystate Website would also have operated as expected on Plaintiff's device during the relevant time period.²⁴

103. The sensitive information exchanged was disclosed along with Private Information regarding Plaintiff, such as her IP address, Facebook ID, and other unique identifiers.

104. Plaintiff was not aware that Defendant was disclosing her Private Information or the contents of her communications with the Baystate Website to Meta and Google and never consented to or authorized such disclosures.

105. Plaintiff was shocked when she discovered the privacy violations and is distressed that Defendant has been disclosing her private information to third parties without her knowledge or consent.

106. Discovery will show that Defendant disclosed the information regarding Plaintiff in exchange for enhanced marketing and analytical services from Meta and Google. Defendant benefitted from Plaintiff's information without ever intending to compensate Plaintiff or to inform her that the disclosures had been made.

107. Defendant violated Plaintiff's rights to privacy in her Private Information and sensitive, confidential medical communications.

108. Defendant's conduct injured Plaintiff and will continue to injure Plaintiff.

²⁴ As noted the reports are incomplete and the absence of the data would not indicate that either the Meta cookies or Google cookies were not operating as expected on a given device.

109. Injuries to Plaintiff are also ongoing because her confidential and private information is now in the hands of Meta and Google who have used the information and can continue to use the information for their own purposes.

CLASS ALLEGATIONS

110. Plaintiff brings claims on behalf of herself, individually, and on behalf of the following:

The Patient Class (or “Class”)

All Persons for whom Defendant possesses Private who, within the statute of limitations, exchanged communications containing Private Information with the Baystate Website.

The Massachusetts Subclass (or “Subclass”)

All Persons in the Patient Class who, within the statute of limitations, were residents of Massachusetts.

111. Excluded from the Class and Subclass are all judges and their staff assigned to this case and any members of their immediate families.

112. Plaintiff reserves the right to redefine the Class and/or divide the Class into subclasses at, or prior to, the class certification stage; in response to discovery; or pursuant to instruction by the Court.

113. This action is properly maintainable as a class action as specifically defined in Massachusetts Rule of Civil Procedure 23.

114. Numerosity: The Class and Subclass are so numerous that joinder of all class members is impracticable. Given the volume of Defendant’s business, there are hundreds or thousands of Class and Subclass members.

115. Commonality: This case presents common questions of law and fact, including but not limited to:

- a. Whether Defendant's practices relating to contemporaneous disclosures of Plaintiff's and Patient Class members' communications with Defendant to Meta and Google attached to Private Information violates the ECPA;
- b. Whether Defendant's practices relating to the disclosures of Plaintiff's and the Subclass members' communications with Defendant to Meta and Google attached to Private Information violates G.L. c. 214, § 1B;
- c. Whether an implied contract exists between Defendant and members of the Class and Subclass;
- d. Whether Defendant's alleged conduct breached the implied contract between Defendant and the Class/Subclass;
- e. Whether Defendant's practices relating to disclosures of Plaintiff's and Class/Subclass members' communications with Defendant to Meta and Google were intentional;
- f. Whether Defendant's conduct harmed and continues to harm Plaintiff and Class/Subclass members, and, if so, the extent of the injury;
- g. Whether and to what extent Plaintiff and Class/Subclass members are entitled to damages and other monetary relief;
- h. Whether and to what extent Plaintiff and Class/Subclass members are entitled to equitable relief; and
- i. Whether and to what extent Plaintiff and Class/Subclass members are entitled to attorneys' fees and costs.

116. Typicality: Plaintiff's claims are typical of the members of the Class and Subclass.

Plaintiff and all members of the Class and Subclass visited the same website, programmed in the

same way by Defendant, and had the same types of information sent to Meta and Google. Plaintiff and all members of the Class and Subclass are patients of Defendant.

117. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class and Subclass because she and her experienced counsel are free of any conflicts of interest and are prepared to vigorously litigate this action on behalf of the Class and Subclass.

118. Questions of law and fact common to the Class and Subclass predominate over any questions affecting only individual members of the Class and Subclass, and a class action is superior to other available methods for the fair and efficient adjudication of this litigation. Defendant's conduct described in this Complaint stems from common and uniform policies and practices, resulting in common violations of the ECPA, the Privacy Act, as well as Defendant's contractual and common law obligations. Members of the Class and Subclass do not have an interest in pursuing separate actions against Defendant, as the amount of each Class and Subclass member's individual claim is small compared to the expense and burden of individual prosecution. Class certification also will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning Defendant's practices. Moreover, management of this action as a class action will not present any likely difficulties. In the interests of justice and judicial efficiency, it would be desirable to concentrate the litigation of all Class and Subclass members' claims in a single forum.

119. Defendant has acted or refused to act on grounds that apply generally to the Class and Subclass such that final injunctive relief is appropriate respecting the Class and Subclass as a whole.

120. In view of the complexities of the issues and the expenses of litigation, the separate claims of individual class members are insufficient in amount to support separate actions.

121. Yet, the amount which may be recovered by individual class members will be large enough in relation to the expense and effort of administering the action to justify a class action. The administration of this action can be handled by class counsel or a third-party administrator, and the costs of administration will represent only a small fraction of the ultimate recovery to be achieved.

COUNT I

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986 (ECPA), 18 U.S.C. §§ 2510 *et seq.* (Plaintiff Individually and on behalf of the Patient Class)

122. Plaintiff incorporates each of the allegations in the preceding paragraphs as if set forth at length herein.

123. The ECPA, 18 U.S.C. § 2511, prohibits the intentional interception of the content of any electronic communications.

124. An individual's communications with a website constitute "electronic communications" as defined by the ECPA, 18 U.S.C. § 2510(12). The communications between Plaintiff and other Class members and Baystate, through the Baystate Website, were electronic communications under the ECPA.

125. The tracking technologies inserted into the hidden code of the Baystate Website, including Google Analytics and Meta Pixel, are "electronic devices" as defined in ECPA, 18 U.S.C. § 2510(5). "Electronic devices" also include (i) any devices Class members used to access the Baystate Website; (ii) Class members' web browsers used to access the Baystate Website; (iii) Baystate's own computer servers; and (iv) the computer servers of third parties such as Google and Facebook which intercepted Class members' communications with the Baystate Website.

126. The computer code for tracking technologies such as Google Analytics, Meta Pixel, and others enabled Google, Facebook, and other third parties to record and disclose to Google, Facebook, and other third parties the contents of communications between Baystate and users of the Baystate Website, including, but not limited to, (i) information about the webpages the user visited; (ii) the precise text of search queries; (iii) the search criteria individuals used to find doctors; and (iv) the precise contents of information the individuals inputted onto forms on the website.

127. As reflected in the facts presented in this Complaint, including a technical analysis of the substance of information intercepted by third parties through the tracking technologies, Baystate configured both its website and the tracking technologies in a manner that revealed the contents of communications between healthcare consumers and Baystate, including by using and permitting the interception of descriptive URLs (URLs that contain words that provide information on the substance of the communication between the consumer and Baystate), permitting the interception of descriptions of services for which patients sought treatment, the substance of requests for information on particular doctors, and interception of the precise words used in searches inputted by healthcare consumers.

128. Baystate also used tracking technologies on pages that would confirm to third parties such as Google and Facebook the user's likely status as Baystate patients, including pages through which patients could make appointments and request medical records.

129. With respect to Plaintiff, the tracking technologies revealed information regarding the doctors, treatments, and patient status for Plaintiff by configuring the tracking technologies to reveal the substance of communications regarding searches for doctors, requests for information

on particular conditions, requests for appointments, and requests for medical records through the patient portal.

130. By inserting the computer code for Google Analytics, Meta Pixel, and other tracking technologies, Baystate intentionally intercepted, endeavored to intercept, and procured another person to intercept the electronic communications of Plaintiff and Class members, in violation of 18 U.S.C. § 2511(1)(a).

131. Additionally, through the above-described tracking technologies, after Baystate intercepted communications, the intercepted information was, in turn, used by third parties, such as Facebook and Google, to 1) place Plaintiff in specific health-related categories based on their past, present, and future health conditions and 2) target Plaintiff with particular advertising associated with their specific health conditions.

132. Baystate facilitated the interception of communications between the Class members and Baystate, and Baystate disclosed such intercepted communications to Google, Facebook, and other third parties without their knowledge or consent. Moreover, their privacy interests were violated by the interception.

133. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

134. Baystate intentionally intercepted the contents of Plaintiff's and Class members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, violation of HIPAA and the FTC Act, as well as the other causes of action set forth in this Complaint.

135. Because of Baystate's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class members' Private Information, Defendant does not qualify for the party exemption.

136. As alleged above, Baystate violated a provision of HIPAA, specifically 42 U.S.C. § 320d-6(a)(3), which imposes a criminal penalty for knowingly disclosing IIHI to a third party.

137. HIPAA defines IIHI as: any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. 42 U.S.C. § 1320d-(6).

138. Plaintiff's Private Information that Baystate disclosed to third parties qualifies as IIHI, and Baystate violated Plaintiff's expectations of privacy and constitutes tortious and/or criminal conduct by violating 42 U.S.C. § 1320d(6). Baystate used the intercepted electronic communications to increase its revenues.

139. The penalty for violating HIPAA is enhanced where "the offense is committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6. Baystate specifically used tracking technologies to intercept and disclose the Private Information of Plaintiff and the Class for financial gain.

140. Baystate's conduct violated 42 U.S.C. § 1320d-6 in that it: (i) used and caused to be used identifiers associated with specific patients without patient authorization; and (ii) disclosed IIHI to Facebook and other third parties without patient authorization.

141. Baystate's conduct is subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Baystate's use of the Facebook source code was for Baystate's commercial advantage to increase revenue from existing patients and gain new patients.

142. The ECPA (18 U.S.C. § 2520(a)) provides a private right of action to any person whose electronic communications are intercepted, disclosed, or intentionally used in violation of the ECPA.

143. Pursuant to the ECPA, Plaintiff seeks for herself and each Class member statutory damages of \$100 for each day of Baystate's violation of the ECPA for Plaintiff and each Class member, or \$10,000 with respect to Plaintiff and each Class member, whichever is higher, plus reasonable attorneys' fees and other litigation disbursements that her counsel has incurred and will reasonably incur in prosecuting this action.

COUNT II

INVASION OF PRIVACY IN VIOLATION OF MA G.L. c. 214, § 1B **(Plaintiff Individually and on behalf of the Massachusetts Subclass)**

144. Plaintiff incorporates each of the allegations in the preceding paragraphs as if set forth at length herein.

145. G.L. c. 214, § 1B provides that "a person shall have a right against unreasonable, substantial, or serious interference with her privacy. The superior court shall have jurisdiction in equity to enforce such a right and in connection therewith to award damages."

146. All health care providers owe their patients a duty not to disclose medical information about the patient without the patient's informed consent.

147. G.L. c. 111, §70E provides that every patient of a Massachusetts health care facility shall have the right "to confidentiality of all records and communications to the extent provided by law."

148. The confidentiality of the patient-provider relationship is a cardinal rule of the medical profession which has come to be justifiably relied upon by patients seeking advice and treatments.

149. Plaintiff and members of the Massachusetts Subclass are patients of Defendant.

150. Defendant owes Plaintiff and members of the Subclass a duty of confidentiality.

151. Despite their duty not to disclose without informed consent, Defendant disclosed information relating to Plaintiff's and Subclass members' medical treatment to Meta and Google without their knowledge or informed consent.

152. The information disclosed includes confidential medical information, including Private Information such as Plaintiff's and Subclass members' status as patients of Defendant, the contents of communications exchanged between Plaintiff or Subclass members with Defendant, details regarding which doctors or support groups Plaintiff or Subclass members scheduled appointments for, and information regarding medical diagnoses.

153. The disclosure of Private Information constitutes an unreasonable, substantial, and serious interference with Plaintiff's and Subclass members' rights to privacy.

154. Plaintiff and Subclass members were damaged by Defendant's violation in that:

- a. Sensitive and confidential information that Plaintiff and Subclass members intended to remain private is no longer private;
- b. Defendant took valuable information from Plaintiff and Subclass members and derived benefit therefrom, including obtaining enhanced advertising and analytics services from Meta and Google, without Plaintiff's and Subclass members' knowledge or informed consent and without sharing the benefits with Plaintiff or Subclass members;

- c. Plaintiff and Subclass members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality. Plaintiff and Subclass members would not have used Defendant's services, or would have paid substantially less for these services, had they known their Private Information would be disclosed.

COUNT III

BREACH OF IMPLIED CONTRACT

(Plaintiff Individually and on behalf of the Patient Class, or in the alternative the Massachusetts Subclass)

155. Plaintiff incorporates each of the allegations in the preceding paragraphs as if set forth at length herein.

156. Plaintiff and the members of the Patient Class sought medical care and information from Defendant through the Baystate Website.

157. In order to obtain medical care and information from Defendant through the Baystate Website, Plaintiff and Class members provided their user data containing Private Information to Defendant.

158. When Plaintiff and Class members exchanged their Private Information in order to obtain information and services from Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information to third parties without their consent.

159. Plaintiff and Class members reasonably believed and expected that Defendant would not disclose their Private Information to third parties because, inter alia, Defendant made numerous promises not to disclose their information without consent and to not use their information for any purposes other than furthering the customer/patient relationship.

160. Plaintiff, and Class members accepted Defendant's offers and provided their Private Information to Defendant in exchange for information and services.

161. Plaintiff and Class members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating itself to not disclose Plaintiff's and Class members' Private Information without their consent.

162. Defendant breached these implied contracts by disclosing the Private Information of Plaintiff, and Class members, to third parties, *i.e.*, Facebook and/or Google, and using it for non-medical purposes, *i.e.*, to obtain enhanced marketing and analytical services.

163. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and the Class sustained damages as alleged herein, including:

- a. Sensitive and confidential information that Plaintiff and Patient Class members intended to remain private is no longer private; and
- b. Defendant took valuable information from Plaintiff and Patient Class members and derived benefit therefrom, including obtaining enhanced advertising and analytics services from Meta and Google, without Plaintiff's and Class members' knowledge or informed consent and without sharing the benefits with Plaintiff or the members of the Class.

164. Plaintiff and Class members are entitled to nominal, compensatory, and consequential damages as a result of Defendant's breaches of implied contract.

COUNT IV

BREACH OF FIDUCIARY DUTY

(Plaintiff Individually and on behalf of the Patient Class, or in the alternative the Massachusetts Subclass)

165. Plaintiff incorporates each of the allegations in the preceding paragraphs as if set forth at length herein.

166. A fiduciary relationship existed between Baystate, a healthcare provider, and Plaintiff and members of the Class, all of whom are Baystate patients. Furthermore, Baystate assumed the role of a fiduciary by undertaking to collect the Private Information of those persons.

167. A fiduciary relationship existed between Baystate, a healthcare provider, and each member of the Class, each of whom is a Baystate patient. Furthermore, Baystate assumed the role of a fiduciary by undertaking to collect the Private Information of the members of the Class.

168. When possessing nonpublic medical information, medical providers such as Baystate have a duty to keep such information completely confidential.

169. Plaintiff and the members of the Class had a reasonable expectation of privacy in the responses and communications entrusted to Baystate through its website, which included highly sensitive Private Information. Baystate's policies bolstered that expectation, given Baystate's promises that Baystate would not disclose communications on the website to third parties.

170. Contrary to its duties as a healthcare provider and its express promises of confidentiality, Baystate installed the tracking technologies to disclose and transmit to third parties the Private Information of Plaintiff and the members of the Class, including information relating to their healthcare.

171. These disclosures were made without the knowledge, consent, or authorization of Plaintiff and the members of the Class.

172. Baystate's secret and unauthorized disclosures of Private Information constituted a breach of Baystate's fiduciary duties to Plaintiff and the members of the Class to safeguard and protect her Private Information.

173. Accordingly, Plaintiff, individually and on behalf of members of the Class, seeks compensatory damages (including damages to compensate for the injuries described herein).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Subclass, asks for judgment in their favor and that the Court award:

- a. Statutory damages of \$10,000 to Plaintiff and Patient Class members pursuant to the ECPA;
- b. Damages for the violation of privacy as to the members of Massachusetts Subclass;
- c. Contract and other damages as to Plaintiff and the members of the Patient Class and Massachusetts Subclass for Defendant's breach of implied contract and breach of fiduciary duties;
- d. Punitive damages in an amount to be determined by a jury;
- e. Attorneys' fees and litigation costs reasonably expended;
- f. Appropriate injunctive relief enjoining the disclosures alleged herein which were made without Plaintiff's and Class members' express, informed written consent or other form of authorization;
- g. Granting such other and further relief, in law or equity, as this Court may deem appropriate and just.

/

/

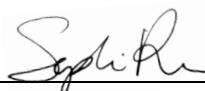
/

JURY DEMAND

Plaintiff, on behalf of herself and the Class and Subclass, demands a trial by jury on all issues triable by a jury.

Date: January 31, 2025

Respectfully submitted,

By: 

Sophia M. Rios (*pro hac vice*)
BERGER MONTAGUE PC
8241 La Mesa Blvd., Suite A
La Mesa, CA 91942
Tel.: (619) 489-0300
srios@bm.net

Sherrie R. Savett
Lane L. Vines
BERGER MONTAGUE PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel.: (215) 875-3000
ssavett@bm.net
lvines@bm.net

Jonathan Shapiro (BBO No. 454220)
Shapiro & Teitelbaum LLP
55 Union Street, 4th Floor
Boston, MA 02108
Tel.: (617) 742-5800
jshapiro@jsmtlegal.com

*Attorneys for Plaintiff
and the proposed Class and Subclass*